CFTC and NFA Cybersecurity- Leveraging Frameworks to Demonstrate Regulatory Compliance

Elizabeth P. Gray, Richard Borden and Paul J. Pantano, Jr.
Willkie Farr & Gallagher LLP

COMING SOON:

Understanding & Avoiding Spoofing Behavior

Spoofing has always been prohibited, but never before has it received such regulatory focus. This course draws on recent cases to cover the basics of spoofing and how regulators are evaluating trading behavior. The course concludes with standard practices for monitoring trading activity.

Topics include: flipping, vacuuming, order splitting and iceberg orders

AVAILABLE COURSES:

- Market Conduct Fundamentals
- Exchange Trading & Regulatory Fundamentals for Electronic Traders
- Key Regulatory & Trading Requirements for Eurex
- Key Features and Regulatory Framework of the London Metal Exchange
- Rules & Regulatory Guidance for CME Group Markets
- Rules & Regulatory Guidance for ICE Futures U.S.
- Safeguarding Customer Funds
- Trade Surveillance & Regulatory Guidance for the Singapore Exchange

For more information, visit FIA.org/Training

Reminders

- The webinar will be recorded and posted to the FIA website following within 48 hours of the conclusion of the live webinar.
- Please use the “question” function on your webinar control panel, at the bottom of your screen, to ask a question to the moderator or speakers.
- CLE certificates will be emailed as soon as approval is received.

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.

What is Cybersecurity?

- Protecting **Confidentiality, Integrity, and Availability** of Information and Information Systems.
- Requires a comprehensive approach across an organization
  - Written policies and procedures
  - Technical measures (firewalls, logs)
  - Security audits, penetration tests, vulnerability scans
  - Employee training

Current State of Play and Trends

Ponemon Institute study indicates the average data breach costs the affected company **$3.86 million**

2020 showed hackers can work from home

- Business email compromise
- Ransomware attacks
- SolarWinds Hack

SolarWinds

"Supply Chain" Attack

- Why is this one so bad?
- NotPetya

Public ramifications

- Approximately $3.5B loss in stock price (about 37%)
- PE Funds have Board Seats
- Lawsuits and Investigations are Inevitable
- Other Software Vendors

Microsoft Exchange

- Hacking campaign found recently in March 2021
- Active exploitation of vulnerabilities in Microsoft Exchange on-premises products

Financial Regulators and Cybersecurity

- Federal and state financial regulators
  - Focused on cybersecurity regulation and enforcement
  - CFTC, FIA, and NYDFS are active leaders in the cybersecurity space
- “My administration will make cybersecurity a top priority at every level of government” – President-elect Biden, Dec. 17th.
- Expect cybersecurity legislation to garner bi-partisan support
  - Different than privacy regulation

CFTC
COMMODITY FUTURES TRADING COMMISSION

FIA

NEW YORK STATE
Department of Financial Services

FIA

Cybersecurity Programs

Based on Standards

- NIST 800-53 rev 5
  - 1,190 Controls
- ISO 27000
  - Similar number

Information Security Organizations use these standards to develop information security policies and procedures

- Information Security Policies are designed to protect the organization
- Information Security Policies are **NOT** designed to comply with regulations

Regulators require demonstration that the Information Security Program complies with regulation

If the organizations does not demonstrate compliance to regulatory auditors, the auditors will make their own interpretations

Preparing For The Audit

A Regulatory Information Security and Privacy Compliance Program is designed to **demonstrate** how the organization identifies regulatory requirements

- And how it's policies and procedures are used to comply with regulation

In the same way that financial controls are documented and tested

- Gather Evidence of the Effectiveness of Cybersecurity and Privacy Controls as they relate to regulatory requirements

How to Translate Information Security Programs into Regulatory Compliance

Use the NIST Cybersecurity Framework (CSF) and Privacy Framework (CPF) as translation devices

- Create **Regulatory** Cybersecurity and Privacy Policies that map to both the underlying Information Security Policies, Privacy Policies and the regulations
- There are crosswalks between the CSF and CPF and NIST 800-53 and ISO 27000
- There are additional crosswalks to SEC Regulations, HIPAA, GDPR, CCPA, etc.
- Primary Information Security and Privacy Controls should be mapped to the applicable regulations and presented to regulators and auditors to demonstrate compliance

NIST Cybersecurity Framework

NIST Cybersecurity Framework Version 1.1 to NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*

Function	Category	Subcategory	NIST SP 800-53, Revision 5 Control
Identify (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization	CM-8
		ID.AM-3: Organizational communication and data flows are	AC-4, CA-3, CA-9, PL-8, SA-17
		ID.AM-4: External information systems are catalogued	AC-20, PM-5, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, RA-9, SA-20, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-2, PM-29

Cybersecurity Program

Develop and adopt a Cybersecurity Program that meets the cybersecurity requirements applicable to the entity.

- Based on cybersecurity security assessments;
- Cybersecurity Program to include written policies and procedures

Example:

[Entity Name]
CYBERSECURITY POLICY

Cybersecurity Program Statement

[XXXXX] ("[XXXXX]" the "Company") is fully committed to information security and legal and regulatory compliance. To that end, the Company has developed and implemented a Cybersecurity Program designed to protect the confidentiality, integrity and availability of the Company's information systems. The Company's Cybersecurity Program is based on, and informed by, periodic information system and cybersecurity risk assessments.

The Company's Cybersecurity Program, Cybersecurity Policy and related policies and procedures are intended to address all applicable regulatory requirements regarding privacy and information security, including the regulations entitled *Cybersecurity Requirements for Financial Services Companies,* 23 NYCRR Part 500, issued by the New York State Department of Financial Services (the "NYSDFS"), and may impose requirements that go beyond those set forth in such regulations.

3. Asset Inventory and Device Management. The CISO (or a designee) shall be responsible for developing and maintaining FGIC's asset inventory and device management processes and procedures. These processes and procedures are set forth in the Procedures.

Cybersecurity Procedures

[XXXXX]
CYBERSECURITY PROCEDURES
Cybersecurity Document Number [ ]

[XXXXX] ("[XXXXX]" or the "Company") is fully committed to information security and legal and regulatory compliance. To that end, [XXXXX] has developed and implemented a Cybersecurity Program (the "Program") designed to protect the confidentiality, integrity and availability of [XXXXX]'s information systems. One component of the Cybersecurity Program is [XXXXX]'s Cybersecurity Policy (as amended from time to time, the "Cybersecurity Policy") which has been adopted by [XXXXX] as of [DATE]. The below Cybersecurity Procedures, as they may be amended or supplemented from time to time (the "Procedures"), supplement the Cybersecurity Policy and are intended to address applicable regulatory requirements under the regulations entitled *Cybersecurity Requirements for Financial Services Companies,* 23 NYCRR Part 500 (the "Regulations"), issued by the New York State Department of Financial Services (the "NYSDFS"). The Cybersecurity Policy, as the same may be amended or supplemented from time to time, is incorporated herein by reference. Capitalized terms used and not otherwise defined herein shall have the meanings ascribed to such terms in the Regulations.

Requirement	Applicable Procedure/Process	Supporting Docs	Regulatory Requirements
I. IDENTIFY (ID)			
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.			
ID.AM-1: Physical devices and systems within the organization are inventoried			

Mapping Cybersecurity Regulatory Requirements

Requirement	Applicable Procedure/Process	Supporting Docs	Regulatory Requirements
I. IDENTIFY (ID)			
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.			
ID.AM-1: Physical devices and systems within the organization are inventoried	[XXXXX]'s CISO (or a designee) maintains a written inventory of information technology infrastructure assets, along with appropriate supporting documentation. Such assets include, but are not limited to, the following: (a) Computers, networking and telecommunications equipment, peripherals, accessories and portable or wireless devices; (b) Software applications, operating systems and development or monitoring tools; (c) Databases, electronic files and records used in IT operations and removable media devices; and Applicable external information systems.		NYDFS 500.03(a)(2)

Additional regulatory requirements (e.g. CFTC, SEC) can be added to the Cybersecurity Procedures as applicable to the entity.

CFTC and NFA Rules and Guidance

CFTC

System safeguards for market infrastructure:

- Designated contract markets (DCMs) (CFTC Rule 38.1051)
- Swap execution facilities (SEFs) (CFTC Rule 37.1401)
- Swap data repositories (SDRs) (CFTC Rule 49.24)
- Derivatives clearing organizations (DCOs) (CFTC Rule 39.18)

System safeguards for intermediaries and advisors (CFTC Rule 160.30):

- Futures commission merchants (FCMs)
- Swap Dealers (SDs)
- Commodity trading advisors (CTAs)
- Commodity pool operators (CPOs)
- Introducing brokers (IBs)

CFTC and NFA Rules and Guidance

CFTC

System safeguards for market infrastructure:

- Designated contract markets (DCMs) (CFTC Rule 38.1051)
- Swap execution facilities (SEFs) (CFTC Rule 37.1401)
- Swap data repositories (SDRs) (CFTC Rule 49.24)
- Derivatives clearing organizations (DCOs) (CFTC Rule 39.18)

System safeguards for intermediaries and advisors (CFTC Rule 160.30):

- Futures commission merchants (FCMs)
- Swap Dealers (SDs)
- Commodity trading advisors (CTAs)
- Commodity pool operators (CPOs)
- Introducing brokers (IBs)

CFTC and NFA Rules and Guidance

(Continued)

MPD (formerly DSIO) Cybersecurity during Coronavirus (COVID-19) Alert, March 19, 2020 — https://www.cftc.gov/media/3666/DSIOCyberAlert031920/download

Gramm-Leach-Bliley Act Security Safeguards, CFTC Staff Advisory No. 14-21, DSIO, February 26, 2014 — https://www.cftc.gov/sites/default/files/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf

NFA

NFA Rules 2-9, 2-36 and 2-49

NFA Interpretive Notice 9070 (Aug. 20, 2015, April 1, 2019 and September 30, 2019) — https://www.nfa.futures.org/rulebook/rules.aspx?RuleID=9070&Section=9

CFTC and NFA Rules and Guidance

(Continued)

NFA Notice I-19-07, Reminder: April 1, 2019 effective date for amendments to NFA's Interpretive Notice regarding Information Systems Security Programs—instructions for notifying NFA of applicable cybersecurity incidents, March 11, 2019 –

https://www.nfa.futures.org/news/newsNotice.asp?ArticleID=5097

NFA Cybersecurity Guidance –

https://www.cftc.gov/About/CFTCOrganization/NFACybersecurityGuidance083118

System Safeguards for Market Infrastructure

When the CFTC adopted final rules clarifying cybersecurity requirements applicable to market infrastructure and establishing new testing requirements, it emphasized that DCM, DCOs, SEFs and SDRs must:

- Be able to “detect, contain, respond to, and recover from cyber attacks;” and
- Follow “generally accepted standards and best practices” to ensure the security of their IT systems.

System Safeguards for Market Infrastructure: Risk Analysis and Oversight

A market infrastructure's risk analysis and oversight program must address:

- Enterprise risk management and governance
- Information security
- Business continuity-disaster recovery planning and resources
- Capacity and performance planning
- Systems operations
- Systems development and quality assurance
- Physical security and environmental controls

Market Infrastructure: Testing Requirements

Vulnerability testing must be conducted:

- At least quarterly for SDRs and covered DCMs, or as frequently as risk analysis indicates;
- By independent contractors or independent employees.

External penetration testing must be conducted:

- At least annually by SDRs and covered DCMs, or as frequently as risk analysis indicates;
- For SDRs and covered DCMs by independent contractors, and for all others by independent contractors or independent employees.

Market Infrastructure: Testing Requirements *(Continued)*

Internal Penetration Testing must be conducted:

- At least quarterly for SDRs and covered DCMs, or as frequently as risk analysis indicates;
- By independent contractors or independent employees.

Controls Testing must be conducted as follows:

- SDRs and Covered DCMs:
  - Independent contractors must test key controls at least every three years;
  - Independent contractors or independent employees must test non-key controls as frequently as risk analysis indicates;
- All other entities may use independent contractors or independent employees to perform controls testing as frequently as risk analysis indicates.

Market Infrastructure: Testing Requirements *(Continued)*

Security Incident Response Plan (SIRP) testing must be conducted:

- At least annually by SDRs and covered DCMs;
- For all other entities, as frequently as risk analysis indicates;
- By independent contractors or employees.

Enterprise Technology Risk Assessment must be conducted:

- At least annually by covered DCMs and SDRs;
- For all other entities, as frequently as risk analysis indicates;
- By independent contractors or employees.

Market Infrastructure: Review, Reporting and Remediation

Senior management and the board of a market infrastructure must receive and review reports setting forth the results of the assessment and testing required by the rule

The level of detailed provided should be sufficient to provide senior management and the board with the ability to conduct effective and knowledgeable oversight of cybersecurity

A market infrastructure must:

- Identify and document and vulnerabilities and deficiencies revealed by its testing program;
- Conduct and document an analysis of any identified risks in order to determine whether to remediate or accept each risk;
- Complete any required remediation in a timely manner given the risks.

System Safeguards for Intermediaries and Advisors

Part 160 of the CFTC regulations establishes 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]."

Rule 160.1 requires financial institutions to provide notice to customers of privacy policies and practices (Rule 160.2 provides model privacy form).

- Must provide initial, annual and revised privacy notice detailing privacy policies and procedures.
- Must provide method for customer to opt out of disclosure to unaffiliated third parties.

Rules limit 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 administrative, technical and physical safeguards for the protection of customer records and information.

The policies and procedures must be 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 records or information that could result in substantial harm or inconvenience to a customer.

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

Designate an employee with privacy and security management oversight

Identify, in writing, all internal and external risks to security

Design and implement safeguards to control the identified risks

Train staff to implement the privacy and security program

Regularly test safeguards, controls, systems, policies, and procedures

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

Engage an independent party to test and monitor safeguards

Oversee service providers with access to customer records and information

Regularly evaluate and adjust the program in light of risks

Design policies and procedures for responding to unauthorized access incidents

Provide the board of directors with an annual assessment of the program

NFA Interpretive Notice 9070 - NFA Compliance Rules 2-9, 2-36 & 2-49: Information Systems Security Programs *(updated Sept. 30, 2019)*

Members have a supervisory duty to assess and prioritize the risks associated with their use of information technology systems

Members should have supervisory practices in place reasonably designed to diligently supervise the risks of unauthorized access to or attack of their information technology systems, and to respond appropriately should unauthorized access or attack occur.

Members have flexibility to design and implement information systems security programs (ISSPs) appropriate for their circumstances.

A Member's ISSP should:

- Establish and implement governance framework that supports informed decision making and escalation within the firm to identify and manage information security risks

NFA Interpretive Notice 9070 (Mar. 1, 2016) *(Continued)*

- Be approved, in writing, by the CEO or other senior officer with responsibility for IT security (*e.g.*, CTO or CISO) or other senior principal with authority to supervise execution of ISSP.
- Inventory critical IT hardware and systems and identify internal and external threats and vulnerabilities
- Document and describe in ISSPs the safeguards deployed in light of the identified and prioritized threats and vulnerabilities (notice provides examples of safeguards)
- Include an incident response plan for managing detected security events or incidents, analyze potential impact and take appropriate measures to contain and mitigate the threat

Members should be familiar with notice requirements U.S. and non-U.S. data security and privacy statutes and regulations

NFA Interpretive Notice 9070 *(Continued)*

The ISSP should contain Member's procedures to restore compromised systems and data, communicate with appropriate stakeholders and regulatory authorities and incorporate lessons learned

- Include procedures to promptly notify NFA of a cybersecurity incident related to the Member's commodity interest business and that results in:
  - any loss of customer or counterparty funds;
  - any loss of a Member's own capital; or
  - in the Member providing notice to customers or counterparties under state or federal law
- Contain a description of Member's ongoing education and training relating to information security for all appropriate personnel

NFA Interpretive Notice 9070 *(Continued)*

Members should:

- Monitor and regularly review the effectiveness of ISSPs, including efficacy of safeguards deployed, and make adjustments as appropriate
- Perform regular review of ISSP at least once every twelve months using either in-house staff with appropriate knowledge or by engaging an independent third-party information security specialist
- Address in their security risk assessment the risks posed by critical third-party service providers with access to a Member's systems, operate outsourced systems for the Member or provide cloud-based services such as data storage or application software to the Member

All records relating to a Member's adoption and implementation of an ISSP and that document a Member's compliance with the NFA's Interpretive Notice must be maintained pursuant to NFA Compliance Rule 2-10

CFTC Enforcement Actions for Cybersecurity Violations

In re Phillip Capital Inc., CFTC Docket No. 19-22 (2019)

In September 2019, the CFTC issued an Order accepting an offer of settlement of, and imposing sanctions against, Phillip Capital Inc. ("PCI"), a registered FCM, for violations of the CFTC's cybersecurity-related regulations.

The CFTC found that PCI violated Regulation 166.3 by failing to supervise diligently the adequate implementation of, and compliance with, policies and procedures related to:

- cybersecurity and PCI's written information systems security program ("ISSP"); and
- unauthorized disbursements of customer funds by PCI's employees as a result of a fraudulent phishing scheme.

In re Phillip Capital Inc. *(Continued)*

The CFTC also found that PCI violated Regulation 155(i) by failing to disclose to its current or prospective customers in a timely manner the material facts of the cyber breach and fraudulent wire transfer.

The CFTC's findings include a long litany of supervisory and disclosure failures by PCI, including:

- Although PCI's IT Engineer was responsible for data and systems issues, vendor management, website maintenance, and data archiving, he had limited training in cybersecurity, and cybersecurity was not broadly within his sphere of responsibility;
- PCI's CCO did not have a background in, or familiarity with, IT generally or cybersecurity specifically and was unable adequately to evaluate the sufficiency of cybersecurity policies and trainings;

In re Phillip Capital Inc. *(Continued)*

- Although PCI's ISSP tracked language in NFA Interpretive Notice 9070, which provides guidance regarding information systems security practices, PCI failed to tailor the ISSP program to its particular business activities and risks;
- When PCI's IT manager resigned, it did not fill the position and, instead, allocated his responsibilities among various employees who were not adequately qualified to manage cybersecurity;
- PCI did not have compliance personnel who could knowledgably assess the adequacy of its policies and procedures relating to cybersecurity;

In re Phillip Capital Inc. *(Continued)*

- When they discovered the cybersecurity breach, none of the involved PCI employees--including the IT Engineer, the two co-CEOs, and the CCO--consulted the ISSP to determine how to respond;
- PCI discovered the unauthorized wire transfer, reimbursed the customer and informed the CFTC. But PCI's management decided not to inform PCI's customers of the cybersecurity breach or the fraudulent wire transfer.
- Moreover, management made concerted efforts to hide the breach from its customers and the public.

In re Phillip Capital Inc. *(Continued)*

The sanctions imposed by the CFTC included:

- a $500,000 civil penalty;
- a $1 million disgorgement order (with a credit for previously returned customer funds);
- a cease and desist order; and
- a requirement to submit a report concerning its improvements to its cybersecurity systems and procedures.

In re The Options Clearing Corporation, CFTC Docket No. 19-19 (2019)

In September 2019, the CFTC issued an Order accepting an offer of settlement of, and imposing sanctions against, The OCC, a registered DCO, for violations of, among other things, the CFTC's system safeguard regulations applicable to DCOs.

The CFTC found that OCC violated Regulations 39.18(b)(1) and (e)(1) by failing to fully establish and maintain a program of risk analysis and oversight reasonably designed to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.

According to the settlement order, OCC failed to establish and maintain policies and procedures that were reasonably designed to:

- consistently identify, prioritize, test, and implement vendor-issued patches; and
- ensure security threats would be promptly detected.

In re The Options Clearing Corporation

(Continued)

The sanctions imposed by the CFTC included:

- a $5 million civil penalty for system safeguard and other violations;
- a cease and desist order; and
- a requirement to retain an independent third party compliance auditor to audit and report on OCC's compliance with, among other requirements, the specified system safeguard requirements.

In re AMP Global Clearing LLC, CFTC Docket No. 18-10 (Feb. 12, 2018)

In February 2018, the CFTC issued an Order accepting an offer of settlement of, and imposing sanctions against, AMP Global Clearing LLC (“AMP”), a registered FCM, for violations of the CFTC’s cybersecurity-related regulations.

The CFTC found that AMP violated Regulation 166.3 by failing to supervise diligently its IT Provider’s implementation of certain provisions in AMP’s written information systems security program ("ISSP"), which resulted in the compromise of customer records and information when AMP’s IT network was accessed by an unauthorized third party.

In re AMP Global Clearing LLC *(Continued)*

The CFTC's findings listed the following, among other, supervisory failures by AMP:

- Contrary to the ISSP, the IT Provider failed to identify, or perform a risk assessment of the remote synchronization port (which permitted unauthorized remote access to AMP's network storage), and failed to identify any network security concerns in its quarterly network risk assessments;
- In April 2017, a third party accessed and copied 97,000 files from AMP's network storage, including customer records and information;
- The failure by AMP's IT Provider to implement fully the ISSP left unprotected against cyber-exploitation a significant amount of customer information, over a multiple month period.

In re AMP Global Clearing LLC *(Continued)*

The sanctions imposed by the CFTC included:

- a $100,000 civil penalty, which reflected credit for AMP's voluntary disclosure to the CFTC of the violation and cooperation with the investigation;
- a cease and desist order; and
- a requirement to submit a report detailing its efforts to maintain and strengthen the security of its network and confirming compliance with its ISSP's requirements.

Thank you to our panelists!

Michael Sorrell
MODERATOR
Deputy General Counsel, FIA

Richard Borden
Counsel, Willkie Farr & Gallagher

Elizabeth P. Gray
Partner, Willkie Farr & Gallagher

Paul J. Pantano, Jr.
Senior Counsel, Willkie Farr & Gallagher

WILLKIE
WILLKIE FARR & GALLAGHER LLP

FIA


FIA