Financial Institutions

Asset Management State of the Market

SEC Focus

Asset management is in a period of rapid change, driven by shifting investor preferences, margin compression, regulatory developments and advancing technologies. Navigating the impact of these disruptive forces and new regulations can be a challenge for asset managers – especially those at smaller firms.

Review our findings for a better understanding of current market trends and how asset managers can adjust accordingly.

Protect the Retail Investor

Share Class Selection Disclosure Initiative

Identify failures to disclose conflicts of interest related to marketing fees and expenses associated with the selection of MF share classes, incentivizing self-reporting.

1. Example: The SEC charged a financial services company, for recommending and selling higher-fee mutual fund shares to retail retirement account customers, for failing to provide sales charge waivers, and for failing to safeguard retail investor assets from theft by its representatives.

Some of the more significant SEC trends and current reporting issues include: revenue and expense recognition problems; faulty valuation and impairment decisions; missing or insufficient disclosures; misappropriation through accounting misrepresentations; inadequate internal controls; and misconduct by financial reporting gatekeepers.

Cyber-Related Misconduct

Identity Theft – Red Flags Rule

Protect investors against identity theft through the disclosure of cyber breaches and violations.

1. Example: A prominent web services provider failed to properly assess the scope, business impact, or legal implications of the largest cyber breach in history, including whether, when and how the breach should have been disclosed ($35 million penalty).
2. Example: The SEC brought settled proceedings against an Iowa-based BD and RIA related to its failures in cybersecurity policies and procedures surrounding a cyber intrusion that compromised the personal information of thousands of its customers.
3. Example: SEC charged a day trader with allegedly participating in a scheme to access the brokerage accounts of more than 100 unwitting victims and make unauthorized trades to artificially inflate the stock prices of various companies.

Digital Assets and Initial Coin Offerings (ICOs)
High-risk "investments." In many cases, issuers lack established track records, viable products, business models, or the capacity to safeguard digital assets from theft by hackers, and some issuers are outright frauds.

1. Example: The SEC charged two co-founders of a purported financial services start-up, who allegedly orchestrated a fraudulent ICO that raised more than $32 million from thousands of investors. Criminal authorities separately charged and arrested both defendants.

Misconduct in Registration, Unregistered Broker-Dealer Activity or Fraudulently Use of Blockchain Technology

1. Example: Two individuals who ran a self-described "ICO Superstore" that operated as an unregistered broker-dealer and participated in unregistered offerings.
2. Example: A hedge fund manager was charged by the SEC with misrepresentations and registration failures, based on its concentration of investments in digital assets.

Leverage SEC Proprietary Technology
to identify insider trading, cherry-picking schemes and the sale of unsuitable investments – exercising their suspended trading authority.

1. Example: For almost three years, an advisor traded securities his firm's omnibus account but waited to allocate the trades to client accounts until after the securities' performance changed over the course of the day. The advisor then "cherry-picked" the trades, disproportionately allocating profitable trades to his accounts and unprofitable trades to his clients' accounts, reaping substantial profits for himself at his clients' expense.

Impose Remedies that Most Effectively Further Enforcement Goals

Focus on Individual Accountability

- In 2018, the SEC charged more than 70% of the individuals in stand-alone enforcement actions. These include CEOs, CFOs, accountants, auditors and other gatekeepers.
- Commission obtained judgments for disgorgement and/or penalties from more than 500 individuals (+9% YOY).

Go Further than Financial Remedies (Disgorgement, Penalties, etc.)

1. Example: A CEO misused her total control to defraud investors
   - Stripped of super-majority voting control – prevented her from ever benefiting from the future sale/liquidation until other shareholders were made whole.
2. Example: A CEO tweeted out false and misleading statements about a purported take-private.
   - Enhancement of corporate governance: Required appointment of two new independent directors, a new committee of independent directors, and for the CEO to step down as chairman, as well as enhanced oversight of CEO's communications.

Our Solutions

Investment Management Liability Solutions

Today's asset managers face an abundance of risks. CNA's specialized industry knowledge and experience meets your clients' evolving and complex needs and helps to alleviate the concern of these risks.

1. Broad definition of claim to include:
   - Informal investigation coverage for all insured persons and internal investigation coverage for executives. No wrongful act is required for either.
   - Formal investigation coverage for insured entities (violations of securities laws/ERISA).
   - Written demands for monetary or non-monetary relief; civil, criminal or regulatory proceedings; requests to toll or waive statute of limitations; alternative dispute proceedings, and extradition.
2. Mock exam reimbursement.
3. Cyber liability (first-party coverage) – Provides $50,000 sublimit for fees and expenses insureds incur in responding to cyber breach. Coverage is intended to be primary over any cyber insurance purchased.
4. Cyber liability (third-party coverage) – Provides a sublimit for claims alleging violation of privacy or unauthorized disclosure of personal information by a client in the course of rendering or failure to render professional services.

Industry-Leading Cyber Risk Control Expertise

CNA Risk Control

CNA is an industry-leading provider of Risk Control services. Our cyber security Risk Control consultants are specialists, averaging more than 20 years of experience in their respected field, and also holding the Certified Information Privacy Technologist (CIPT) designation. The CIPT is achieved by demonstrating an understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.

Further, only CNA offers the expertise of Underwriter's Laboratories (UL) Recognized Risk Engineers, individuals who have been certified by UL, a world leader in advancing safety. CNA's UL Recognized Risk Engineers blend insurance coverage knowledge with risk management principles to build customized Risk Control solutions for our clients.

- Cyber hotline: 800-247-3968
- Email: cyberintake@cna.com

eRisk Hub

CNA cyber policyholders receive access to eRiskHub®, an online web portal powered by NetDiligence®, loaded with tools and resources to help them understand their exposures, respond effectively and minimize the effects of a breach on their organizations.

Registration instructions are provided with your CNA Cyber policy. If you have any questions please contact your CNA Cyber underwriter.

Preferred Pricing Arrangements

Post breach vendors and additional vendors.

- Legal counsel – "breach coach"
- Forensic investigation
- Notification
- Credit monitoring
- Public relations

CNA Net Protect® for Financial Institutions

With CNA NetProtect® for Financial Institutions, your clients have access to underwriting expertise and risk management strategies that combine people, controls, technology and insurance into a comprehensive insurance solution. It's designed to address both first- and third-party risks, and it sets a high industry standard for network security, content and privacy liability.

Asset Manager Fidelity Bond Enhancement Rider

Client Capital

This coverage is designed to protect against loss of clients' funds as a result of dishonest or fraudulent acts committed by an employee when the insured is acting as a fiduciary. The definition of client is broadly defined to include organizations or individuals who have an account with the insured, are in the process of opening an account with the insured, or have been informed and reasonably believe that an employee of the insured has opened or is in the process of opening an account on their behalf with the insured.

Cyber Crime

1. Computer-to-computer systems fraud
    - Misappropriated access credentials: Loss from a customer's account resulting from the direct unauthorized access of the insured's computer through the use of the misappropriated customer access credentials.
    - Hacker, interloper or virus: Loss resulting from the fraudulent transfer of money or uncertificated securities from the insured's account caused directly by the unauthorized entry of data or computer programs into the insured's computer by a hacker, interloper or virus without the use of access credentials, thereby causing the computer to effect such transfer.
2. Fraudulent transfer instructions – funds transfer fraud: Loss resulting from an employee having transferred money, securities or uncertificated securities from a customer's account in reliance on a fraudulent instruction transmitted to the insured via the insured's online banking system, facsimile device, telephone or email.
3. Data or computer systems destruction or theft: Loss resulting from malicious modification, manipulation, destruction of, or damage to data or computer programs owned by the insured or for which the insured is legally liable as well as loss resulting from the robbery, burglary, larceny, theft, misplacement or mysterious unexplainable disappearance of data or computer programs owned by the insured or for which the insured is legally liable.

For more information, contact your CNA underwriter or visit cna.com/financialinstitutions.