Proskauer Built to Serve Asset Managers

Current Enforcement and Compliance Considerations for Asset Managers

June 30, 2020

Legal & Business
Insights for Asset Managers
The Bottom Line

A Proskauer Webinar Series

Speakers

Thomas Brown
Managing Director,
Berkeley Research Group, LLC
T: +1 646 862 0979
tbrown@thinkbrg.com

William Komaroff
Partner, Proskauer
T: +1 212 969 3975
wkomaroff@proskauer.com

Don B. Melamed
Partner, Proskauer
T: +1 310 284 5621
dmelamed@proskauer.com

Seetha Ramachandran
Partner, Proskauer
T: +1 212 969 3455
sramachandran@proskauer.com

Hadassa R. Waxman
Partner, Proskauer
T: +1 212 969 3040
hwaxman@proskauer.com

Proskauer

Cybersecurity & Privacy: Compliance and Risks

Proskauer

Scope of the Cybersecurity Threat

- Cyber attacks are widespread, systemic and difficult to detect.
- Entities across all sectors may be targeted for financial, political or ideological reasons or for bragging rights.

Who’s Doing the Hacking?

- Outsiders
  - Financially motivated cybercriminals
  - “Hacktivists”
  - Hackers for hire
  - Nation-state-supported actors
- The careless or malicious insider

How a Breach Happens

- Exploitation of Network Vulnerabilities
  - Mismanaged computer systems
  - “Zero-day” vulnerabilities
- Social Engineering
  - “Phishing” attacks
- Physical Devices
- DDoS Attacks
- Misuse of Permissions

Cyber Attack Outcomes

- Data Breaches
  - Consumer financial data
  - Proprietary information
- Ransomware
- Wire Transfer Fraud
  - Business email takeovers

Key Consequences

- Direct Financial Loss and Costs of Responding to an Attack
- Reputational Harm
- Disruption of Business Operations
- Private Civil Litigation
  - Consumer class actions
  - Shareholder or derivative actions
  - Financial institutions (if card/bank data compromised)
- State, Federal and International Enforcement Actions
  - DOJ/SEC/FTC/FINRA
  - States Attorneys General
  - CCPA
  - GDPR
- Intellectual Property Theft
- Compliance Costs

Statutory and Regulatory Framework

- Graham Leach Bliley Act of 1999
  - Requires federal agencies to establish standards to safeguard security and confidentiality of customer records.
    - Treasury Department, Federal Reserve, FDIC issued Interagency Guidelines Establishing Information Security Standards for banking institutions.
    - SEC issued the “Safeguards Rule” (Regulation S-P).
      - Applies to brokers, dealers, investment companies, and registered investment advisors.
      - Requires written policies and procedures reasonably designed to (a) ensure confidentiality of customer records and (b) protect against any anticipated threats or unauthorized access of customer information.
    - FTC has its own version of the Safeguards Rule

Statutory and Regulatory Framework

- SEC Disclosure Guidance
  - February 2018: Commission issued a statement emphasizing that cybersecurity presents ongoing risks to companies and markets.
  - October 2018: SEC issued a report looking at factors it would consider to determine whether businesses violated the federal securities laws by failing to have a sufficient system of internal controls to prevent losses from BEC and similar schemes.
  - In short, having insufficient internal controls resulting in losses from a cyberattack could result in issues with the SEC.

Statutory and Regulatory Framework

- FTC Act's Prohibition on Unfair and Deceptive Practices
  - Prohibits "unfair or deceptive acts or practices" in or affecting commerce.
  - FTC has used a deception theory to allege that businesses failed to live up to their stated data security practices.
  - FTC has also used an unfairness theory based on businesses failure to employ "reasonable and appropriate measures to prevent unauthorized access to personal information."

Statutory and Regulatory Framework

- State Data Breach
  - Almost all of the states require private entities to notify individuals of security breaches of information involving “personally identifiable information.”
  - California now has a private right of action permitting victims of identity theft to bring a cause of action against a business for failure to protect their PII.
  - States’ Attorney Generals can impose penalties on companies for failure to protect PII.

A Global Approach to Cyber Risk

- Develop and implement a **comprehensive information security plan**.
- Once implemented, plan should be **reviewed and updated regularly**.
- There should be **clear lines of communication and authority** for cyber security within the organization.

A Global Approach to Cyber Risk

- Companies should consider at least the following:
  - **Cyber Risk Assessment**
  - Cyber Governance Committee
  - **Cyber Incident Response Plan**
  - Chief Information Security Officer
  - Cyber Insurance Policies
  - Recurrent Security Audits
  - Culture of Security

Cyber Risk Assessment

- Identify internal and external threats.
- Review computer network and identify/assess vulnerabilities. For example:
  - Are software patches applied in a timely fashion?
  - Is the network adequately segmented?
  - Are access controls sufficient?
  - Is data encrypted where necessary?
  - Are network logs appropriately detailed and maintained?
  - Is the network topology map up to date?
- Review vendor relationships (esp. data storage vendors). For example:
  - Do they have cyber risk protocols?
  - Do my clients require me to have cyber risk protocols?

Cyber Incident Response Plan

- Elements of a basic plan
  - Make sure one person “owns” cyber security and reports directly to the Board.
  - On-call independent third-party investigators/forensic experts
  - Consider privilege
  - Restoration of system integrity
  - Brand protection
- Coordinate with regulators and law enforcement agents.
  - Develop blue-sky relationships
  - Consider law enforcement referral option

What to Do If You Are Hacked?

- Speed is important
- Engage counsel/legal quarterback
- Bring in independent experts
  - Define scope of the problem
  - Evidence collection
  - Mitigation plan
- Consider law enforcement referral

Final Thoughts – The Bottom Line

- Cyber security is a business risk, not an “IT problem.”
- Should be managed and mitigated like any other risk.
- This is a long-term process.

False Claims Act

Proskauer

Civil False Claims Act

- Law dates back to Civil War era
  - Aimed at combating fraud and abuse in federal government programs
- Cases can arise in any situation involving federal government spending
- Historically common in:
  - Healthcare
  - Government contracts and procurement
- CARES Act relief programs likely to spur substantial growth in cases
  - Significant attention being put on FCA as a means of addressing abuse

Civil False Claims Act

- Liability based on knowingly or recklessly submitting a false claim to the government
  - Specific intent to defraud not required
  - Preponderance of the evidence standard
- Cause of action on behalf of the government
  - DOJ initiated
  - Relator initiated via Qui Tam action
- Remedies include treble damages and attorneys fees for relator's counsel

Civil False Claims Act

- Implications for recipients of CARES Act or other government funds
  - Risk of hindsight analysis
  - Whistleblowers / Qui Tam actions
- Portfolio company level risk
- Asset manager level risk
  - Greater involvement in portfolio company management = greater risk of legal exposure

Civil False Claims Act

- The Bottom Line – To Mitigate Risks
  - Contemporaneous documentation
  - Rigorous internal controls
  - Training and compliance programs
  - Effective Whistleblower programs

Anti-Money Laundering ("AML")

Money Laundering Examples

- Using a shell company to disguise the origin or ownership of the funds
- Facilitating a financial transaction while remaining willfully blind to the source of the investor's assets or the nature of the investor's transactions
- Sending money out of (or receiving money in) the U.S. to conceal the source of money you know (or should know, but are taking steps to avoid learning) to be the proceeds of a crime, and thereby make it less accessible to creditors
- Advising a customer on how to structure a transaction to avoid reporting requirements

Bank Secrecy Act ("BSA")
31 U.S.C. §§ 5311-5330

- Enacted in 1970, originally intended as a tool to fight tax evasion and organized crime
- Amended by USA PATRIOT Act in 2001
- Requires that “financial institutions” have an effective AML program
- Criminalizes willful failure to have an effective AML program
- Definition of “financial institution” is steadily expanding
- Both criminal and civil penalties, which vary by statute
  - Criminal penalties can include up to ten years imprisonment plus $500,000 fine
  - Civil penalties (up to twice the amount of the laundered proceeds)
  - Forfeiture of assets is another potential consequence of violating BSA

Covered “Financial Institutions”

- Banks
- Broker-dealers
- Mutual Funds
- Any entity requires to register under the Commodities Exchange Act
- Insurance Companies
- Most FinTech Companies
- Casinos
- Money Service Businesses (Western Union, Moneygram, Walmart)
- Credit card companies, Sellers and Providers of “Prepaid Access”
- Dealers in precious metals or stones

Emerging Areas of AML Regulation

- Real estate businesses
- Auction houses, galleries – fine art and antiquities

The SEC's Authority to Pursue SAR Violations

- FinCEN has the authority to enforce the BSA, but the SEC regularly brings enforcement actions against broker-dealers for failing to file SARs.
- In 2017, the SEC filed an enforcement action in the SDNY against Alpine Securities. Alpine objected to the SEC's authority to pursue the action, arguing that the SEC does not have the authority to enforce the BSA.
- The court found that SEC's Rule 17a-8, which requires broker-dealers to comply with certain BSA regulations, gave the SEC "independent authority to require broker-dealers to make reports" and "enforcement authority over those broker-dealer reporting obligations."

Compliance Programs are Critical

- Low legal threshold for imposition of corporate criminal liability
- BSA requires:
  - System of internal controls to ensure compliance
  - Designated individual responsible for compliance
  - Training of appropriate personnel
  - Independent testing for compliance

Compliance Programs are Critical (cont'd)

- Customer Due Diligence Requirements for Financial Institutions ("CDD Rule")
  - Identify and verify identity of customers;
  - Identify and verify the beneficial owners of (i.e., the humans behind) legal entity customers;
  - Understand the nature and purpose of customer relationships; and
  - Conduct ongoing monitoring to maintain and update customer information and to identify suspicious transactions.

Relevant Agencies

- Department of Justice
- FinCEN – Financial Crimes Enforcement Network
- New York State Department of Financial Services
- OCC – Office of Comptroller of the Currency
- Federal Reserve Bank
- FDIC

Office of Foreign Assets Control ("OFAC")

Proskauer

Office of Foreign Assets Control ("OFAC")

- Part of Treasury Department
  - 31 C.F.R. §500-598
- Administers laws imposing economic and trade sanctions against
  - Foreign countries, territories and governments
  - Entities
  - Individuals

Office of Foreign Assets Control ("OFAC") (cont'd)

- OFAC List of Specially Designated Nationals ("SDN List")
  - A list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries
  - U.S. persons are prohibited from engaging in any transactions with SDNs and must block any property in their possession or under their control in which an SDN has an interest
- OFAC Sectoral Sanctions Identification List ("SSI List")
  - U.S. persons are not required to block the property of individuals and entities on SSI lists (unless the targets are also on the SDN list), but other prohibitions and investment restrictions apply

OFAC Sanctions and Enforcement

- OFAC Sanctions Programs apply to ALL U.S. PERSONS
  - U.S. citizens and permanent resident aliens, regardless of where located
  - All non-U.S. citizens located in the United States
  - Entities organized under U.S. law
  - Foreign branches or offices of U.S. entities
  - In some instances, foreign companies owned or controlled by U.S. persons, such as a foreign subsidiary of a U.S. parent
    - E.g., Cuba and Iran sanctions

Criminal and Civil Penalties

- TWEA (Trading with the Enemy Act)
  - Authorizes the use of economic sanctions against foreign nations, citizens and nationals of foreign countries
- IEEPA (International Emergency Economic Powers Act)
  - Authorizes the president to regulate commerce after declaring a national emergency in response to any unusual and extraordinary threat to the United States which has a foreign source
- CISADA (Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010)
  - CISADA implementing regulations issued by OFAC — Iranian Financial Sanctions Regulations

U.S. Sanctions
SDN/SSI Compliance Consideration

- OFAC's 50% rule
  - Sanctions apply to persons named on the SDN and SSI lists, their property and their interests in property, including their 50% or more owned subsidiaries
    - Entities owned 50% or more in the aggregate by entities on the SDN or SSI list will also be subject to sanctions, even if such entities are not on the SDN or SSI List
      - Aggregation does not "cross-pollinate" the SDN and SSI Lists

U.S. Sanctions

SDN/SSI Compliance Consideration (cont'd)

- Timing is everything
  - U.S. persons must report to OFAC any blocked or rejected transactions within 10 business days
    - Crucially important to elevate sanctions issues to the legal-compliance department, as quickly as possible

Export Controls

- Bureau of Industry and Security (BIS) – counterpart to OFAC, within the Commerce Department
- Jurisdiction over goods and technology that was developed in the U.S.
- The “Entity List” – similar to OFAC lists, in that export of U.S. goods and technology is restricted.
- E.g., Huawei

U.S. Sanctions Programs

- Venezuela
- Russia
- Iran
- North Korea
- Cuba
- Turkey

- **Global Magnitsky Sanctions**
- **Cybersanctions**

Final Thoughts – The Bottom Line

- AML and OFAC risks are related, but raise distinct legal issues that each need to be addressed as part of an effective compliance program.
- Need to think comprehensively about areas of the business where AML and OFAC risks can come up, and not simply screen names through a filter.
- Have a policy and make sure you follow it.

Proskauer» Built to Serve Asset Managers

Legal & Business Insights for Asset Managers

The Bottom Line

A Proskauer Webinar Series