SEC'S 2018 EXAM PRIORITIES REFLECT CONTINUED FOCUS ON CYBERSECURITY

Annually, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") publishes its examination priorities for the new year. Recently, OCIE announced five priorities that will inform its examinations moving in to 2018.

OCIE is committed to "promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy." In support of these "pillars," OCIE intends to focus on:

1. Issues of importance to retail investors, such as fee disclosures, mutual funds, and exchange- traded funds;
2. Entities that are critical to the proper functioning of capital markets, such as clearing agencies and national securities exchanges;
3. Oversight of the Financial Industry Regulatory Authority (FINRA) and the Municipal Securities Rulemaking Board (MSRB);
4. Cybersecurity; **and**
5. Anti-money laundering programs.

The emphasis on cybersecurity is not new. As early as 2014, OCIE highlighted its commitment to monitoring cybersecurity practices of regulated entities when it launched a series of examinations to identify cybersecurity risks and assess cybersecurity preparedness in the securities industry. In 2015 and 2017, the SEC released the results of its first two cybersecurity examination sweeps. Prior examination priorities also included the SEC's commitment to "examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls at broker-dealers and investment advisers."

In this year's announcement, OCIE noted that the scope and severity of risks related to data breaches and cyber attacks have increased and that such attacks can affect not only the targeted firms, but unsuspecting investors and market participants as well.

In evaluating firms' cybersecurity programs and potential enforcement referrals, the agency intends to emphasize:

- Governance
  - SDDco Regulatory Services, LLC coverage establishes customized policies and procedures that describe and evidence proper governance controls over data and data security.
- Risk assessments
  - SDDco Regulatory Services, LLC coverage includes cybersecurity risk assessments, data handling assessments, email vulnerability testing, and infrastructure testing including endpoints and full external penetration tests.
- Access rights and controls
  - SDDco Regulatory Services, LLC develops full policies and procedures including data access privileges. Coverage also includes electronic endpoint diagnostics along with other tools to ensure compliance with policies and procedures.
- Data loss prevention
  - SDDco Regulatory Services, LLC develops full policies and procedures including data handling. Coverage also

  - includes electronic endpoint diagnostics along with other tools to ensure compliance with policies and procedures.
- Vendor management
  - SDDco Regulatory Services, LLC provides and produces full third party rostering and vendor due diligence along with vendor agreements.
- Training
  - Armor customizes and provides multiple actively managed and ongoing data security training and testing for all designated individuals.
- Incident response
  - SDDco Regulatory Services, LLC trains and educates personnel to recognize exposure incidents and provides incident reporting from within the client dashboard. SDDco Regulatory Services, LLC then activates full response management including containment, planning, investigations and determination of state, federal, notifications and corrective actions.

As noted in a recent post, cybersecurity continues to be a top priority for the SEC's Division of Enforcement as well. Indeed, in 2017 the Enforcement Division created a new specialized "Cyber Unit" dedicated to investigating violations related to cybersecurity intrusions and breakdowns. And the SEC's Chairman, Jay Clayton, has made clear in public remarks that he is personally focused on the issue. Unfortunately, these public statements provide little specific guidance as to what cybersecurity measures will be deemed adequate. Whether specifically subject to OCIE's examination authority or not, however, organizations should be mindful that the SEC's spotlight on cybersecurity is likely to intensify and approach their own risk assessments, budget, resources, and compliance priorities accordingly.