MILNE LEGAL | ML

JANUARY 14, 2016

Milne Legal Press Release

Cybersecurity Remains a SEC Priority in 2016

I. Cybersecurity: Be Prepared for a SEC Examination

On January 11, 2016, the U.S. Securities and Exchange Commission ("SEC") announced its "Examination Priorities for 2016".[1] As expected, similar to 2015, Cybersecurity risks remains a top priority for SEC examinations in the New Year. In this announcement, the SEC stated that it will advance its examination efforts in 2016 by testing and making assessments of investment advisers and broker-dealer's implementation of its cybersecurity procedures and controls.[2]

To be prepared for an examination, investment advisory and broker-dealer firms registered with the SEC must not only have written policies and procedures in place to adequately address cybersecurity risks, but the firm's IT infrastructure must also be properly set up and tested and its employees sufficiently trained how to prevent and respond to potential cyber attacks.

ML has partnered with a local IT company in Zürich to help its client's have written policies and procedures on cybersecurity, and to perform tests on the effectiveness of its IT systems.

---

[1] See the following link on the SEC's website: https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf

[2] Id.

Dustin W. Milne
Managing Partner

"Working together with our IT partner in Zürich (or with a firm's existing IT service provider), we can help ensure that our clients don't suffer from any disconnect between the firm's written cybersecurity policies and procedures and the firm's actual IT systems designed to prevent and detect cybersecurity threats.

It is our experience that chief compliance officers appreciate the employee IT training we provide and our testing of the effectiveness of the firm's IT system."

The SEC's has set forth measures that investment advisory firms should consider in addressing cybersecurity risks, including the following:

(i) Conduct a periodic assessment of the technology system the firm uses;
(ii) Create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses; and
(iii) Implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures. Firms may also wish to educate investors and clients about how to reduce their exposure to cybersecurity threats concerning their accounts.[3]

The SEC's Chair, Ms. Mary Jo White, highlighted the SEC's concerns:

> *"Cybersecurity threats know no boundaries. That's why assessing the readiness of market participants and providing investors with information on how to better protect their online investment accounts from cyber threats has been and will continue to be an important focus of the SEC. Through our engagement with other government agencies as well as with the industry and educating the investing public, we can all work together to reduce the risk of cyber attacks."*

---

[3] See the SEC's Division of Investment Management's Guidance Update, issued in April 2014,: https://www.sec.gov/investment/im-guidance-2015-02.pdf

Beginning right where it left off in 2015, the SEC continues to send a clear message to registered investment advisers and broker-dealers that they must have adequate cybersecurity policies and procedures in place and such policies must be tested by the firm for effectiveness.

II. The SEC's First Cybersecurity Enforcement Action.

On September 22, 2015, the SEC brought its first enforcement action against an adviser for failure to adopt proper cybersecurity policies and procedures prior to the actual cyber-breach taking place.

This enforcement action highlights the SEC willingness to bring enforcement actions against an investment adviser even though no client had been financially harmed.

The SEC made the following statement:

> *"Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."*[4]

The SEC's order found that the adviser violated Rule 30(a) of Regulation S-P (commonly referred to as the "Safeguards Rule") under the Investment Advisers Act of 1940. Generally speaking, the Safeguards Rule requires registered investment advisers to adopt written policies and procedures reasonably designed to protect customer records and information. Therefore, when it was discovered that the adviser had not adopted adequate policies and procedures to protect against this cyber attack, the SEC concluded that the adviser had violated federal securities law, i.e., the Safeguards Rule, although no financial harm to the advisory clients was found:

> *"As we see an increasing barrage of cyber attacks on financial firms, it is important to enforce the safeguards rule even in cases like this when there is no apparent financial harm to clients"*[5]

---

[4] Statement made on September 22, 2015, by Marshall S. Sprung, Co-Chief of the SEC Enforcement Division's Asset Management Unit.

[5] Id.

III. Conclusion

The SEC is sending its registrants an unequivocal message that cybersecurity remains a hot topic in the New Year and the implementation of such policies and procedures will be closely scrutinized under examination. We can arrange for an assessment of your existing policies and cyber security protections.

Charles Lerner

Laetitia Mantel

"We recommend that every registered investment adviser and broker-dealer, led by the firms' chief compliance officers, have effective cybersecurity policies and procedures to guard against cyber attacks.

The effectiveness of the policies and procedures and your IT process should be tested on a periodic basis as well as employees should receive adequate cybersecurity training.

With our IT partner located in Zürich, Switzerland (or by working with the firm's existing IT provider), we can ensure that our clients have effective IT systems which provide appropriate protections, and train the firm's employees on how to detect and properly respond to cybersecurity threats."

* * * *

Mr. Milne can be contacted at: dustin.milne@milnelegal.com

Mr. Lerner can be contacted at: charles.lerner@milnelegal.com

Ms. Mantel can be contacted at: laetitia.mantel@milnelegal.com