

## Sehr geehrte Kunden

*Willkommen zu unserem Quartals-Newsletter, der einige der wichtigsten Aktualisierungen und Nachrichten der SEC in Bezug auf die Schweiz enthält.*

*Am Dienstag, 21. September 2021 hielten wir eine Präsentation vor der Swiss Registered Investment Advisor Association (SRIAA) im Baur au Lac. Es war schön, uns endlich wieder einmal treffen zu können. Die Präsentation, die als Referenzdokument gedacht ist, vergleicht und kontrastiert den U.S. SEC und den neuen Schweizer Regulierungs- und Compliance-Rahmen und ist hier abrufbar.*

## Allgemeine Updates

### 1. Aktuelle Themen laut der Investment Advisors Association 2021

Laut der kürzlich veröffentlichten Umfrage zum Thema Compliance-Tests in der Vermögensverwaltung 2021, die hier abrufbar ist, ergab die Befragung von 350 RIA-Compliance-Beauftragten folgende Themenbereiche., welche Ihnen am meisten Sorgen bereiten::

1. Advertising und Marketing an erster Stelle;

Dicht gefolgt von:

2. Cybersecurity

Dann, in keiner besonderen Reihenfolge:

3. Climate change and ESG
4. Business Continuity Planning
5. Digital Assets

## 2. Cybersicherheitsmängel - Fälle zum ersten Mal eingereicht

Im letzten Newsletter haben wir uns eingehend mit digitalen Vermögenswerten, Kryptowährungen und Krypto-Assets befasst. Diesmal können wir berichten, dass die SEC tatsächlich mit der Durchsetzung der Cybersicherheit auf einer Einstiegsstufe beginnt. Bis zu diesem Sommer hatte die SEC in Bezug auf die Durchsetzung nicht viel Bemerkenswertes getan. Im August änderte sich dies mit drei separaten Verfahren, an denen insgesamt acht Firmen beteiligt waren.

Bei den acht Firmen, die RIAs, Broker-Dealer und doppelt registrierte Unternehmen umfassen, wurden mangelhafte Cybersicherheitsrichtlinien und -verfahren (P&P) festgestellt, und sie wurden wegen Verstößen gegen Reg S-P angeklagt. Bei zwei der Firmen wurde festgestellt, dass sie gegen die Advisers Act-Regel 206(4) -7 verstossen haben, die sich auf die Pflicht bezieht, Kunden über einen Verstoß zu informieren.

Der Grund für die Anklage gegen die Firmen war das Versäumnis der Firmen, Cybersicherheits-P&P anzunehmen und umzusetzen, die „angemessen“ sind, um Kundendaten zu schützen. Die betroffenen Firmen waren Ziel eines erfolgreichen Cyberangriffs, bei dem die E-Mail-Konten von Firmenmitarbeitern beeinträchtigt wurden, was dazu führte, dass die persönlichen Daten von Tausenden von Kunden in jeder Firma offengelegt wurden. Die Leiterin der Cyber-Einheit der SEC-Durchsetzungsabteilung, Kristina Littman, erklärte: „Es reicht nicht aus, eine Richtlinie zu verfassen, die verbesserte Sicherheitsmassnahmen vorschreibt, wenn diese Anforderungen nicht oder nur teilweise umgesetzt werden, insbesondere angesichts bekannter Angriffe“. Sie sagte, es handle sich im Wesentlichen um ein Umsetzungsproblem, da die Informationen nicht in einer Weise geschützt wurden, die mit der Firmenpolitik vereinbar war. Hätten die Unternehmen das getan, was sie in den Geschäftsplänen versprochen hatten, wäre es wahrscheinlich nicht zu den Verstößen gekommen.

## Die Lehre daraus ist:

1. Umsetzen, was in den P&P steht,
2. Schnelles Reagieren, wenn ein Verstoss entdeckt wird.

Beides haben die Firmen offensichtlich nicht getan. Es gab Verzögerungen sowohl bei der Reaktion als auch bei der Benachrichtigung der Kunden, was das Problem noch verschärfte.

## 3. Fokus auf Cybersecurity durch die Division of Examinations

In Fortführung des Themas Cybersicherheit wurde in den DOE-Prüfungsprioritäten 2021 ausdrücklich darauf hingewiesen, dass die DOE prüfen wird, ob die Unternehmen geeignete Massnahmen ergriffen haben, um:

- Kundenkonten zu schützen
- den Einbruch in Konten zu verhindern
- Böartige E-Mail-Aktivitäten zu bekämpfen
- Auf Vorfälle zu reagieren

Zu diesem Zweck hat die DOE den Vorgang eingeleitet. Das Schreiben der DOE vom 5. August 2021 listet 33 Punkte auf, die sie sehen wollen, um eine Überprüfung der Cybersicherheit durchzuführen.

Einige der wichtigsten Forderungen aus dem Sweep Exam Letter sind:

1. Richtlinien und Verfahren in Bezug auf die Datenklassifizierung
2. Richtlinien und Verfahren in Bezug auf die Verschlüsselung von Daten

in Bewegung, sowohl intern als auch extern, und von Daten in Ruhe auf allen Systemen und Servern

6. Liste der Systeme, Hilfsprogramme und Werkzeuge, die zur Verhinderung, Erkennung und Überwachung von Datenverlusten eingesetzt werden, einschließlich einer Dokumentation, die ihre Funktionen beschreibt und angibt, ob es sich um proprietäre oder von Dritten verwaltete Systeme oder kommerzielle Standardprodukte handelt
7. Richtlinien und Verfahren, die Folgendes regeln:
  - Verhinderung des Zugriffs von Unbefugten auf Netzwerkressourcen und -geräte
  - Einschränkung der Benutzer
  - Aktualisierung der Zugriffsrechte
  - Einholung der Zustimmung des Vorgesetzten zu Änderungen
  - Laufende Überprüfungen, um sicherzustellen, dass die Zugriffsrechte korrekt zugewiesen werden
  - Liste von Protokollen und Berichten zur Überprüfung von fehlgeschlagenen Anmeldeversuchen, Zugriffsabmeldungen, ruhenden Benutzerkonten und unbefugten Anmeldeversuchen
  - Liste von Drittanbietern mit Zugang zum Netzwerk, zu Systemen oder Daten
8. In Bezug auf die Verordnung S-ID:
  - a. Risikobewertung in Bezug auf abgedeckte Konten
  - b. Richtlinien und Verfahren zur Einhaltung der Verordnung S-ID
  - c. Jährlicher Bericht in Bezug auf die Verordnung S-ID
  - d. Schulungen für Mitarbeiter und Auftragnehmer
  - e. Umgesetzte Änderungen am Programm zum Identitätsdiebstahl
9. Kopie des schriftlichen Plans zur Abschwächung der Auswirkungen

eines Cybersicherheitsvorfalls und/oder zur Wiederherstellung, falls ein solcher Plan existiert

10. Liste aller Cybersicherheitsvorfälle oder -verletzungen

Insgesamt ein bemerkenswert umfangreicher und deutlicher Beweis dafür, dass die SEC die Cybersicherheit in der Praxis immer ernster nimmt.

## 4. Das Moratorium für Neuregistrierungen in der Schweiz

Ende Juni wurde uns mitgeteilt, dass das Moratorium aufgehoben sei. Eine Woche später wurden wir darüber informiert, dass das Moratorium nicht aufgehoben worden war.

Wie wir inzwischen alle wissen, hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) am 25. Juni ein 16-seitiges Memorandum an die SEC geschickt, in dem er seinen Standpunkt darlegt und grünes Licht für die Veröffentlichung von Informationen gibt.

Die SEC antwortete Ende August mit den Worten:

*„Wir betrachten das Memorandum des EDÖB, das sich mit dem Schweizer Datenschutzgesetz befasst, als einen positiven Schritt. Wir gehen davon aus, dass andere schweizerische Gesetze angesprochen werden müssen, um zu bestätigen, dass Antragsteller mit Sitz in der Schweiz in der Lage sind, der Kommission umgehend direkten Zugang zu ihren Büchern und Aufzeichnungen zu gewähren und sich nach der Registrierung einer Inspektion und Prüfung vor Ort zu unterziehen.“*

Der EDÖB hat unseres Wissens nicht formell geantwortet. Auf Anfrage teilte er jedoch informell mit, dass er nach einer endgültigen Stellungnahme seinen Zuständigkeitsbereich ausgeschöpft habe und weder eine Genehmigung erteilen noch eine formelle Bestätigung ausstellen könne. Sollte die SEC weitere Fra-

gen zum Datenschutz haben, werde er natürlich gerne helfen, aber ansonsten sei die Angelegenheit abgeschlossen.

Fazit: Soweit wir wissen, warten wir auf die Rückmeldung der SEC. Wir werden weiter informieren, wenn wir Neuigkeiten erhalten..

## 5. Whistleblower Awards

Obwohl dies für die Schweiz nicht sehr relevant zu sein scheint, dachten wir, dass es sich trotzdem lohnt, dieses Thema aufzugreifen, da es zu den Dingen gehört, an die wir normalerweise nicht denken. Wir finden es interessant und informativ, einen Einblick zu bekommen, wie sich die Dinge in den USA derzeit entwickeln.

Das Whistleblowing-Geschäft boomt in den USA.

Am 15. September gab die SEC zwei Belohnungen bekannt, die eine in Höhe von ca. 110 Mio. \$ für einen Whistleblower und die andere von 4 Mio. \$ für einen anderen Whistleblower. Dies für Informationen und Unterstützung, die zu erfolgreichen Klagen bei der SEC und damit verbundenen Verfahren führten. Damit wurden bisher insgesamt über 1 Milliarde Dollar an 207 Hinweisgeber gezahlt. 500 Millionen Dollar davon wurden allein im Jahr 2021 ausbezahlt, was zeigt, wie sehr dieses Programm an Fahrt aufnimmt. Die höchste Einzelauszahlung an eine Einzelperson erfolgte im Oktober 2020 in Höhe von 114 Millionen Dollar.

Angesichts der Aussagen des SEC-Vorsitzenden Gary Gensler

*„Das Whistleblower-Programm hat seit seiner Einführung vor einem Jahrzehnt massgeblich zum Erfolg zahlreicher Durchsetzungsmaßnahmen beigetragen“*

und

*„Die Unterstützung durch Whistleblower ist entscheidend für die Fähigkeit der SEC, die Regeln für unsere Kapitalmärkte durchzusetzen“,*

sowie die Aussage des SEC-Direktors der Abteilung für Durchsetzung, Gurbir S. Grewal,

*„Das Whistleblower-Programm hat seit seiner Einführung vor einem Jahrzehnt zum Erfolg zahlreicher Durchsetzungsmaßnahmen beigetragen“, wird dies höchstwahrscheinlich fortgesetzt.*

Die SEC hat ein eigenes „Office of the Whistleblower“ mit einem eigenen Leiter,

der für die Überwachung des Programms zuständig ist.

## 6. Compliance Company Market

Dies ist ein Artikel, den wir einfach aufnehmen mussten. Ja, es gibt einen Markt für gebrauchte Compliance-Unternehmen. Noch kann man sie nicht auf eBay kaufen, aber es scheint ein aufstrebender Markt zu sein. Laut Grandview Research lag der weltweite Markt für ausgelagerte Compliance im Jahr 2020 bei einem Gesamtumsatz von rund 6,3 Mrd. US-Dollar, wobei bis 2028 ein Wachstum auf 97,3 Mrd. US-Dollar erwartet wird, was einer durchschnittlichen Wachstumsrate von 13,7% entspricht.

Private-Equity-Firmen und private Fondsberater haben die Chance erkannt und begonnen, sich an Compliance-Unternehmen zu beteiligen. Offenbar hat es inzwischen mindestens ein Geschäft im Wert von über 1 Milliarde Dollar gegeben, und mehrere Geschäfte bewegen sich im Bereich von 10 bis 50 Millionen Dollar.

Dies scheint auf den Druck der Regulierungsbehörden und das daraus resultierende Wachstum in der Branche zurückzuführen zu sein. Die SEC scheint die Outsourcing-Firmen recht wohlwollend zu betrachten, insbesondere für kleine und mittlere RIAs, da die SEC es als ein Zeichen dafür betrachtet, dass die RIAs die Einhaltung der Vorschriften ernst nehmen und einen externen Anbieter beauftragen, um die Lücken zu schließen. Da es sich dabei um eine optionale Ausgabe seitens der RIA handelt, zeigt dies, dass diese zusätzliche Sorgfalt walten lassen.

### Impressum

Aviolo Compliance Solutions GmbH · Seefeldstrasse 94 · CH-8008 Zürich · Switzerland  
Tel.: +41 (0) 44 552 03 87 · Email: [info@aviolo.ch](mailto:info@aviolo.ch) · [aviolo.ch](http://aviolo.ch)