Quarterly Newsletter – Q1 2022

Dear Client

Welcome to our regular quarterly newsletter. Yes, we know, there was no Q4 2021 newsletter. This was because after a year like 2021, nobody seemed to want to read another end of year newsletter any more than we felt like writing one. It is however a long one, lots of news.

On that note, a thought going into the year:

> *"For the Unlearned, old age is winter*
> *For the Learned, it is the season of the harvest"*

- THE TALMUD

1. Cooperation with Bratschi Law

Aviolo Compliance Solutions and Bratschi Ltd. (www.bratschi.ch) are entering into a cooperation to jointly provide integrated legal, regulatory and compliance services. Bratschi is a full service law firm with seven offices all over Switzerland and roughly 100 lawyers. The intent is to bridge the gap between legal advice and the operational implementation of compliance solutions.

A frequent feedback we receive as compliance specialists is about the disconnect between legal advice (interpreting the law) and operational implementation (developing policies, procedures, tasks & activities) in regulatory & compliance matters. Integrating a compliance practice into a law firm has been done very successfully by some medium sized U.S. law firms. A good example in the U.S. is Seward & Kissel LLP (www.sewkis.com), who have integrated a compliance practice into the firm, "Seward & Kissel Regulatory Compliance". This appears to work very well, with clients valuing the close coordination between legal and compliance.

In Switzerland, the financial services act and the financial institutions act (FinSA & FinIA) are driving growing demand for broad and integrated Legal & Compliance services. Up to now there have been distinct break points in the progression between legal frameworks and compliance tasks and activities. With the introduction of the rafts of legislation in recent years, we see it as having become a continuum. Over the next few years, we intend to jointly become one of Switzerlands leading providers of integrated legal, regulatory & compliance services.

Benefits to Clients

- Integrated provision of a full range of legal, regulatory and compliance services
- Operational implementation of legal advice into compliance frameworks in the form of policies, procedures, operational guidelines, controls and checks
- A one stop shop, single point of contact to coordinate work product, transactions, activities across the spectrum
- Ongoing monitoring and review of compliance frameworks at legal oversight and operational levels

The intent is to provide full coverage of legal, regulatory and compliance services across the full continuum of legal advice through to operational implementation at a practice level.

2. General news & updates

1. SEC Proposes New Cybersecurity Rules

The SEC is proposing new cybersecurity risk management rules, including changes that would require both advisors and funds to create policies and procedures "reasonably designed to address cybersecurity risks," according to the commission. This mandates Advisors to create written policies and procedures intended to address cyber risks that could harm clients.

> "Registered investment advisors, investment companies, and business development companies currently have to comply with various rules that may implicate their cybersecurity practices, such as books-and-records, compliance, and business continuity regulations" SEC Chair Gary Gensler said about the proposed rules. Going on to say, "Today's release builds upon those requirements."

The new rules would require additional record-keeping obligations for both advisors and private funds, and would demand advisors confidentially report certain „significant" cyber incidents to the SEC. They would also demand that advisors and funds disclose certain types of cybersecurity incidents to clients and investors.

While advisors currently have to provide disclosures on practices, fees, risks and conflicts as a part of their Form ADV, the new rules would amend the form's Part 2A to require advisors disclose cybersecurity risks and incidents. Gensler intent with this is for the reforms to lower the risk cybersecurity poses to all registrants.

In the proposed rule, the SEC defines a „significant" cyber incident as one that "disrupts or degrades the advisor's ability... to maintain critical operations" that could lead to substantial harm to the advisor or clients. If an advisor can't use

their internal computer systems because of a malware shutdown, for example, that may impair their ability to provide client services, perhaps for days or weeks. Significant harm to a client is one which leads to "significant monetary loss or the theft of personally identifiable or proprietary information," according to the SEC.

The commission's proposal requires firms to report these breaches to the SEC within 48 hours to help monitor the effects on the advisor and clients. On the basis that a number of similar complaints in a short time frame could also indicate a broader, systemic problem.

The proposed rules will be published both on the SEC site and in the Federal Register, and the public comment period will be open for the longer period of 60 days following its publication on the site or 30 days after its publication in the Register.

2. Insider Trading

The SEC has a well-known focus bordering on obsession with insider trading, exemplified by numerous enforcement actions. Highlighting the need for ongoing training and awareness of the risks associated with what the SEC considers material, non-public information. Which we may add, may vary wildly with what FINMA or others consider material non-public information. For us, it's the SEC's opinion that counts, because they have the broadest interpretation of what insider trading and what the use of material, non-public information consists of.

The SEC uses advanced technology that analyses trading patterns, family trading, offshore transactions, focusing on the activities of access persons and related persons.

For an advisor, we strongly recommend, if not in place already, to:

- Maintain and monitor restricted lists for securities
- Know who your corporate insider (and related) clients are and in which companies
- Monitor employees and review unusually profitable trades
  - » In particular, ask the question, "what was the rationale and the research behind a particular unusually profitable trade?"
- Lastly, document everything, everything, everything

We have two examples of the lengths to which this is going, at two extremes.

The first ever "Shadow Trading" case.

This "first ever", "shadow trading" case is currently being prosecuted by the SEC and has been getting quite some airtime. The SEC is saying that Matthew Panuwat, a former business development executive at Medivation Inc, a small Biotech company, on learning in 2016 that Pfizer Pharmaceuticals was about to buy Medivation, bet on further acquisitions by buying the stock of another, rival company, Incyte Corp. Ie., Panuwat bought the stock of a competitor company on the basis of information affecting his own company. "Shadow trading" is the term being used to describe the situation where corporate insiders with non-public information trade in competitors' or supply chain partners' stock to evade insider trading prohibitions. After a few stops and starts as the parties argued back and forth over fact, form and substance, weighed and tested their armaments, sorry, arguments, the case is going forward.

The SEC is arguing "misappropriation theory". However, misappropration theory in this case apparently hangs on Medvation's own policies and procedures which prohibit company executives from trading in "another public company". To be fair, the facts and circumstances don't look good for Panuwat who as it turns out is a former investment banker who, as the SEC is arguing, knew full well that Medivation's sale would raise the Incyte stock price and he acted on that information before the material piece of information, that Pfizer was going to buy Medivation, became public.

In a 14 page decision dated January 14th, U.S. District Judge William Orick denied Panuwats motion to dismiss the case. Stating:

> "Although unique, the SEC theory of liability falls within the contours of the misappropriation theory and the language of the applicable law", Orrick writes.

Referring to the Exchange Act's anti-fraud provisions, Orrick adds:

> "...the SEC's reading of Sec. 10(b) and the regulations is more persuasive than Panuwats.
> Sec. 10(b) and rule 10(b)5 cast a wide net, prohibiting insider trading of any security using any manipulative or deceptive device."

This is one side of the enforcement coin. For completeness, at the risk of appearing politically biased (I'm not), I want to point out another one.

Nancy Pelosi, Trader of the year.

Nancy Pelosi, speaker of the house of representatives (and Rep. for San Francisco) and her husband Paul Pelosi report trades of tens of millions of dollars of assets a year. The Nancy Pelosi Portfolio Tracker, based on the Speakers reported trades, estimates marked outperformance. In 2020 the Pelosis beat the S&P 500 by almost 15%. In 2021, "The Gov Portfolio", a model portfolio based on Nancy Pelosis' trading, followed by 60,000 users (Yes, 60,000 people are apparently mirroring or at least following the speaker of the houses' trading), based on the end-of-year data, made over 40% in total returns, beating the S&P 500 by 28.7% and the Nasdaq 100 by 26.6%.

Nancy and Paul Pelosi have a history of market outperformance going back to the mid 90's following Nancys' election to congress in the late 80's. In 2009 the Pelosis' net worth was estimated at 58 Million USD. In 2014 that had risen to 101 Million USD. As of 2021, Pelosi's net worth was valued at $120 million, making her the 6th richest person in Congress.

While Pelosi was working on anti-trust legislation to regulate the tech industry, the couple were actively trading tech stocks. In May and June 2021, Paul Pelosi traded tech stocks (with a liberal use of options – calls and puts) including Alphabet, Amazon, and Apple, realising gains of 5.3 Million USD. This trading has

been noted, extensively commented on, but has not, to date, been investigated.

In fairness, this is a recognised, general problem across political parties which the STOCK Act of 2012 was supposed to stop or at least curtail. It's unusual that a case this egregious turns up. Most representatives seem to know when to stop.

The take-home message is: unless you are a member of congress in the United States of America, be really, really careful about personal trading. Document everything and when in doubt, don't make the trade.

3. The Moratorium on new registrations in Switzerland – Update

In the wake of the 16 page memo from the Swiss Federal Data Protection and Information Commissioner (FDPIC) to the SEC from 25. June 2021 outlining their position and giving the go-ahead for information to be passed to the SEC there has mostly been radio silence on all sides. Punctuated by the occasional "No Comment" from the SEC.

There has been some conjecture as to what is holding things up. Article 271 of the Swiss Criminal Code being considered by some as the leading contender for the continuing block. It's not.

We wrote to the SEC, asking for clarity. The SEC, Division of Examinations wrote back to tell us that the SEC staff is engaged with FINMA on the matter and suggested reaching out to FINMA.

On reaching out to FINMA, we received a quite helpful response containing the following quote:

> "Any solution found by the SEC and FINMA would be based on art. 42 et seqq. FINMASA and be applicable for RIAs based in Switzerland and authorized by FINMA."

It turns out then that the matter is currently with FINMA. With an ongoing dialogue taking place between the SEC and FINMA to solve it. The issue, apparently, being Article 42 of the Financial Market Supervision Act (FINMASA) – Administrative Assistance (Amtshilfe). Specifically Art. 42c - Informationsübermittlung durch Beaufsichtigte.

Article 42c FINMASA enables supervised institutions (including asset managers) to transmit non-public information to foreign authorities and entities without having to obtain official authorisation. FINMAs interpretation of Article 42c FINMASA is in Circular 2017/6 Direct transmission. FINMA also publish a list of foreign authorities for which the requirements of confidentiality can be assumed to be met. The SEC is on this list. The puzzle for us is why the lengthy discussions? The framework for transmitting information would appear to be relatively clear, with, presumably, precedent.

In closing, for interest, here are the official numbers for new non-domestic RIA applications approved by the SEC, by jurisdiction, for 2021:

United Kingdom:	17
Australia:	4
Bermuda:	1
Bolivia:	1
British Virgin Islands:	1
Canada:	12
China:	1
Hong Kong:	5
India:	1
Ireland:	1
Mexico:	1
United Arab Emirates:	1

Obviously, there was a queue in the UK, which makes sense, the moratorium was lifted for the UK in September 2020, so there was a backlog. Hence the spike in new registrants.

From the data then, there does not appear to be any restrictions on international registrations. Other countries appear free to register. Just not Switzerland, out in the cold. Exile on Main Street.

4. Whistleblowers – the SEC and the EU take on the matter

We touched on this from the SEC viewpoint in the Q3 2021 newsletter. With the coming implementation of the EU Whistleblowing Directive, this is going to become a whole lot more relevant for Switzerland in the next few years. The full text is here.

This has gone somewhat under the radar up to now. However, a recap; the EU Directive is intended to provide common minimum standards of protection across the EU to whistleblowers who raise breaches of EU law with their employer. Regardless of where that employer is actually located. The new rules will require the creation of safe channels for reporting both within an organisation and to public authorities. There are already a number of companies jumping on this bandwagon selling systems which provide such safe channels, eg., Convercent (www.convercent.com), Navex Global (www.navex.com) plus others, with no doubt, more to come.

Specifically, this is a Directive, not a regulation, therefore it presents a series of requirements with the onus on each EU member state to transpose into local law, deciding by themselves how to meet the requirements. As with most laws coming from the EU in the last twenty years, we can reasonably expect Switzerland being forced to follow suit and having to implement something similar. With the usual three to five year time lag.

December 17, 2021 was the deadline for implementation by EU member states and it is enforceable for organizations with 250 or more employees. The next deadline is December 17, 2023, on which the law becomes enforceable for organizations with 50 or more employees.

The Directive requires that companies provide internal mechanisms for whistleblowing. That companies educate employees and others about their whistleblowing options, protect whistleblowers who report breaches of EU law and prevent retaliation. It also includes certain requirements, including establishing external reporting channels.

What this seems to mean, in practice, is that any company based in or with a subsidiary in the EU meeting the 50 employee threshold will be subject to this. In the longer term, we can expect the introduction of something similar in Switzerland as pressure from the EU builds. As usual.

3. Swiss compliance news

The registration and licensing of asset managers with FINMA is proceeding. Not at the fast pace FINMA would like, but it is proceeding. From the FINMA webside as of March 13th 2022 we see that 109 portfolio managers and trustees have been licensed by FINMA and are monitored by a supervisory organization: (https://www.finma.ch/~/media/finma/dokumente/bewilligungstraeger/pdf/vvtr.pdf).
Among these 109 institutions, there are a number of trustees. One of these is also licenced as an asset manager. A further 78 portfolio managers and trustees have been licensed and supervised by FINMA as domestic group companies under the FinIA: (https://www.finma.ch/~/media/finma/dokumente/bewilligungstraeger/pdf/grfinig.pdf).

This is a total of 187 to date. Apparently 2,521 IAMs and Trustees have registered on the FINMA EHP survey and application platform with the intent to register and obtain a license. It follows that FINMA estimates having to process 2,521 applications. (see: Licensing as a challenge and as a seal of quality)

Given that 187 out of 2,521, or just 7.4% of the total have processed to date (from the figures published), and we are entering Q2 of 2022 with the deadline being end of year 2022, with presumably 2,334 to process between now and December 31st, one senses a certain nervousness from the regulator.

One would guess that not all those who have registered on the EHP platform will in fact proceed. Notwithstanding, FINMA expects the volume of applications to reach its highest level in the second half of 2022. Which would presumably indicate that these financial institutions will be being processed by FINMA well into 2023. Well past the deadline. Realistically, we would not be surprised if this continued into 2024.

Many IAMs and particularly trustees find themselves somewhat challenged by the new rules. The rules impact the organisation, internal structures, require-

ments, own funds, they include rules/codes of conduct, such as on dealing with risks from cross-border business, suitability, or market conduct. New ground for many.

All risks emanating from the business must be assessed, estimated, mitigation strategies developed (and documented), then monitored by means of appropriate processes and controls. FINMA focusses on the risks from cross-border business, which can be significant. The financial institutions themselves are responsible for appropriately managing these risks.

FINMA will want to see in the licence application evidence of the required expertise and any necessary adjustments to the organisation. The separation of risk management and internal control from the operational side of the business may also be required from financial institutions below the threshold values as set out in Article 26 FinIO. This will be triggered if the financial institution runs a high-risk business model. For many, it's a lot of new requirements to deal with.

In closing, many AMs (and trustees) are considering outsourcing the compliance and risk function completely. Many are already on the way to doing so. Going forward into the world of FinIA and FinSA, partly or fully outsourced integrated compliance solution may become the preferred solution for small to medium sized institutions. As a compliance firm, with our partners, we are working to help our clients meet the coming challenges.

Impressum

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