Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Annual Media Conference, 27 march 2018

Mark Branson
Chief Executive Officer

Technology and the financial industry – opportunity or risk?

Ladies and Gentlemen

Today I will talk to you about technology, its opportunities, and risks. Blockchain, ICOs, big data and cyber risk are familiar buzzwords. But what lies behind the headlines?

Low interest rates, changing consumer behaviour and low profitability have rendered innovation an urgent, perhaps even existential, issue for the financial industry.

Innovation cannot be prescribed by the state – the industry itself has to step up and innovate. But we as a supervisory authority do have a role, in ensuring that the regulatory framework makes technological advancement possible. This does not mean orchestrating innovation. It means removing barriers to entry for the sake of healthy competition.

However, encouraging innovation does not mean that we are starry-eyed. Digitalisation and innovation in financial services entail new risks, or familiar risks in new guises. Our job is to identify and monitor the risks, and where required, to step in. We are speaking, for example, about money laundering risks in blockchain technology, or the losses that investors might suffer in ICOs, and, in particular, cyber risks.

FinTech's promise

First, though, the opportunities. New products and applications are emerging. Projects are being financed through crowdfunding, payments are being made by smartphone, new strata of society in developing countries are gaining access to financial services, and robots are making investment decisions.

We recognise the potential that FinTech and blockchain technology offer to the Swiss financial services industry. We have repeatedly demonstrated our commitment to innovation. FINMA regulations is technology-neutral. In other words, we make no distinction between digital and analogue channels. It was FINMA that came up with the ideas for the regulatory sandbox and the dedicated FinTech licence. And we have recently issued guidelines for ICO operators.

Laupenstrasse 27
3003 Berne
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

We want to see healthy competition through innovation, but not at the cost of the integrity of the Swiss financial sector. We are as passionately anti-crime as we are pro-innovation.

Blockchain: just hype, or a driver of innovation?

Blockchain is an exciting technology. Parts of today's financial market infrastructure might one day become obsolete. Remember Bill Gates' prediction in 1994 that "Banking is necessary, banks are not".

The technology is best-known as the basis for cryptocurrencies and ICOs. In a short space of time ICOs have gone from being a relatively unknown phenomenon to being a money magnet, raising over six billion dollars worldwide in 2017 alone. Four of the six largest ICOs in 2017 took place in Switzerland, which has become a hub for the industry. No wonder we have been flooded with enquiries about how our rules apply to ICOs leading us to issue guidelines on how we will handle such requests, based on our interpretation of existing regulation.

Initial feedback has been encouraging. Serious service providers have welcomed our approach. They are aware that the vision of a vast anarchic playground is unsustainable.

For despite the excitement, there is no question that cryptocurrencies are risky. A totally permissive approach would be wrong. Fluctuations in value have been extreme, and the risks entailed in ICOs are often not transparent. Information about projects can be rudimentary, and as with other start-up investments, the promised returns may fail to materialise. Then there's the potential for money laundering. Anonymity and lack of transparency are, after all, prized by some cryptocurrency providers. Cryptocurrency trading platforms have also been the victims of major hacker attacks with losses in the hundreds of millions. Our approach is simple: ICOs offering payment tokens are subject to the anti-money laundering regulation, while those offering investment opportunities fall under securities law.

Cyber-risks: FINMA's expectations

The subject of hacking leads us to the topic of cyber-risk for financial institutions. Financial institutions are a target much favoured by hackers and the perpetrators of cyber-attacks. MELANI, the Swiss Reporting and Analysis Centre for Information Assurance, reports that two-thirds of the incidents targeting critical infrastructure in 2017 occurred in the financial sector.

The risks connected with these attacks are growing in sync with the pace of global digitalisation. Cyber-attacks are now the most serious operational hazard facing the financial system, and both the private sector and public authorities should take them extremely seriously. On the whole, the institutions we supervise are aware of the risks and seem well-equipped to deal with them. A large number of attacks are successfully repelled every day, for example, the roughly 100 attacks per day on e-banking systems by so-called "Retefe" malware.

Of course, the best defence is only as strong as the weakest link. For instance, hackers broke into the SWIFT international payments system through successfully targeting the central bank of Bangladesh. In Switzerland, a large volume of customer data was recently stolen from a health insurer.

In light of these risks, what are FINMA's expectations? First, it is essential that financial institutions understand where they are vulnerable. Here penetration tests are an essential instrument. Equally important in the event of a cyber attack is crisis response. Speedy re-establishment of operational functionality is vital. Each institution must develop and test a crisis contingency plan.

However, the risks involve more than simply the theft of money or data. Targeted attacks, perhaps even perpetrated by terrorist, state or state-related sources, could assume systemic dimensions. Although Swiss financial institutions appear individually well-prepared by international comparison, we are doing less than other countries to protect the system as a whole. Other countries with important financial centres do more, for example by setting up cybersecurity competence centres or imposing system-wide penetration tests. Switzerland should follow suit by enhancing its system-wide monitoring and response processes. Here FINMA is ready to play its role. We have recruited specialists in this area and are prepared to make further investments.

In this connection the Advisory Board for the Future of the Financial Centre, chaired by Professor Aymo Brunetti, made three key recommendations that received little attention – wrongly so.

These were, firstly, that access to MELANI should be extended, also to small financial institutions in Switzerland. Secondly, that cooperation between financial sector experts and the authorities should be institutionalised and reinforced. Cyber-risk prevention is one area where the interests of the industry and the supervisor certainly coincide. And thirdly, a cybersecurity crisis response plan for the financial sector needs to be designed and tested.

FINMA welcomes and supports these recommendations. Working together achieves more than going it alone. Switzerland is responding to the threat – but other countries are doing more.

Concentration risk in outsourcing

The ever more prevalent phenomenon of outsourcing, where institutions externalise business processes or their IT infrastructure to an outside provider, has also somewhat increased the potential impact of cyber-attacks.

The majority of Swiss banks have outsourced major business processes. Some banks have outsourced their entire back offices. This outsourcing raises new challenges for supervisory authorities.

In particular, we see a high degree of concentration among certain service providers in Switzerland. A large number of banks outsource their services to the same providers. We expect to see here the same standards as at the financial institutions themselves. Since 2016, we have been legally entitled to conduct on-site inspections of these outsourcing partners, and have begun to carry out systematic checks.

Take the opportunity, but know the risks

FinTech has a lot of potential. As a supervisory authority we will do what we can to facilitate innovation in the financial services industry. That allows the market and, ultimately, the customer to decide whether which applications of the new technology deserve to succeed – not regulation.

We have a heady mixture of innovators, copy-cats, regulatory arbitrageurs and fraudsters in the cryptoworld. It's our job together with our partner authorities to try and make sure that the innovators have the chance to thrive if their idea is worth it, that the arbitrageurs have nothing to gain, and that the fraudsters end up where all fraudsters should.

Not only the risks, but also the opportunities, new technologies provide require our full attention and commitment.

Thank you for listening.