INVESTOR CLAIMS, REGULATORY ENFORCEMENT AND CRIMINAL PROCEEDINGS WITHIN THE FRAME OF INITIAL COIN OFFERINGS

by Nicolas Ollivier[1]

INTRODUCTION

In 2017, the number of Initial Coin Offerings (ICOs)/token-generating events (TGEs) exploded in Switzerland, surpassing and disrupting traditional venture capital investment. Switzerland, and in particularly its renowned Crypto Valley, has emerged as a global hub for ICOs[2]. Under current Swiss law, there is no specific investor protection around ICOs. ICO organizers and their related set-up companies (charitable foundations or other corporate companies registered in Switzerland) are however not untouchable. Civil claims, criminal proceedings, and Swiss Financial Supervisory Authority (FINMA) investigations may be initiated against them. The initiation of such actions may prove to be more complex than for matters unrelated to the blockchain technology in particular due to the challenge for traditional principles of jurisdiction posed by the existence of the decentralized ledger and the possible use of anonymity though encryption. Despite that fact and that there is no relevant case law and consistent legal doctrine yet, the existing Swiss legal framework provides some room for investors to initiate legal actions.

Jamie Dimon, CEO of J.P. Morgan Chase, a staunch Bitcoin critic, recognized that underlying blockchain technology is real and stated that ICOs must be evaluated on a case by case basis[3]. Some believe that history repeats itself and compare the craze to the era of the dotcom boom in the 90s[4].

New opportunities arise with blockchain and smart contracts. It may greatly benefit society at large with numerous advantages, such as self-enforceability, reduced transaction costs, faster settlements and nearly an infinite amount of new decentralized applications. The announcement by Kodak and Telegram of their ICOs early in the year received a surge of enthusiasm. However, in the world of ICOs, many ICOs organizers are proponents of a libertarian view advocating the principle that “code is law” and considering that an ICO is an easy means to raise swiftly and millions of capital without granting any rights to the investors and outside of any

---

1 Nicolas OLLIVIER is a Counsel at LALIVE with offices in Geneva and Zurich. Mr. OLLIVIER can be contacted at nollivier@lalive.ch.

2 PwC report, https://cryptovalley.swiss/wp-content/uploads/20171221_PwC-S-CVA-ICO-Report_December_final.pdf.

3 https://www.cnbc.com/2018/01/09/jamie-dimon-says-he-regrets-calling-bitcoin-a-fraud.html?view=story&%24DEVICE%24=native-android-tablet.

4 See for example William Mougayar, Why The Blockchain Is The New Website, https://www.forbes.com/sites/valleyvoices/2015/12/21/why-the-blockchain-is-the-new-website/#683b7de44dc3.

legal constraints. In this context, the temptation is compelling for ICO organizers to take out the money and abandon the advertised blockchain project, without risking the capital and working long hours.

FINMA'S STANCE TOWARDS ICOs AND ENFORCEMENT PROCEEDINGS

The Swiss Financial Market Supervisory Authority (FINMA) communicated its support to the innovative potential of blockchain technology for the Swiss financial center[5]. From a regulatory perspective, FINMA treats ICOs depending on the functionality of the coin/token (payment tokens, utility tokens, asset tokens, and hybrid tokens) and the ICO set-up so as to determine whether or not the project requires a FINMA license and/or is subject to Anti-Money Laundering (AML) regulations. FINMA published its practice by way of guidelines on 16 February 2018. These guidelines reflect the stance taken by FINMA to treat ICOs, notably which prerequisites are necessary for an ICO not to qualify as security and not be subject to AML Regulation[6].

Although FINMA supports and participates in the federal government's Blockchain/ICO Working Group[7], it stated that some ICO activity may prove to be fraudulent and warned investors in this respect as well as the high price volatility of the coins generated in ICOs projects which are at an early stage of development[8].

In September 2017, FINMA closed down three companies with connection with the QUID PRO QUO Association which issued so-called "E-Coins", a fake cryptocurrency developed by the association itself. Of the four million Swiss francs invested by several hundred users/investors, FINMA was able to seize assets of approximately two million Swiss francs[9]. The deceived users/investors may now only contemplate recovering a part of this amount in proportion to their claim at the end of the bankruptcy proceedings.

FINMA has also stated that it is investigating a number of ICO cases to determine whether regulatory provisions have been breached[10]. Any person, in particular deceived investors, may notify FINMA of ICOs that breach regulatory law. FINMA may thus initiate enforcement proceedings. Informants do not have the right to be kept informed of the opening and progress of the FINMA's investigation. Nevertheless, FINMA must protect

5 FINMA Guidance 04/2017, Regulatory treatment of initial coin offering, 29 September 2017.

6 FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 16 February 2018.

7 https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/?pk_campaign=News-Service&pk_kwd=FINMA%20publishes%20ICO%20guidelines.

8 FINMA Guidance 04/2017, Regulatory treatment of initial coin offering, 29 September 2017.

9 https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter.

10 https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter.

creditors and investors when initiating regulatory scrutiny and deciding which enforcement measures to take, such as precautionary measures, action to restore compliance with the law, confiscation/ordering the disgorgement of profits, and liquidation and bankruptcy[11]. FINMA also publishes notices about statutory liquidations, resolution and bankruptcy proceedings it conducts and supervises on an ongoing basis.

Within the frame of a liquidation/bankruptcy, creditors (including deceived investors who incurred losses) may file a claim to participate in the distribution of the available assets among the recognized creditors.

When FINMA confiscates/orders the disgorgement of profits, investors and creditors have no right of restitution of their assets based on financial market laws. They are only entitled to the recovery of undisputed or legally recognized civil law claims[12]. Furthermore, Art. 35(5) of the Financial Market Supervision Act (FINMA Act) provides that the criminal law confiscation under Art. 70-72 of the Criminal Code takes precedence over confiscation under this provision.

For these reasons and the absence of status of party in the enforcement proceedings (in particular allowing the access to the file), deceived investors should not only contemplate notifying misconduct in the frame of an ICO to FINMA but also evaluate whether a criminal complaint should/may be filed, and/or civil action initiated.

CRIMINAL COMPLAINT

An ICO consists in issuing coins/tokens on a protocol (such as Ethereum) and offering these coins/tokens to investors in exchange of cryptocurrency (generally bitcoins or ethers) or less frequently fiat money.

The ICO craze has attracted many scammers and criminals. The Securities and Exchange Commission (SEC)'s new Cyber Unit announced on 4 December 2017 that it took its first action against a fraudulent ICO since its formation in September. The SEC charged a Canada based cryptocurrency company with ICO fraud and obtained an emergency freezing order to halt the operation. The SEC's criminal complaint sought permanent injunctions, disgorgement plus interest and penalties[13].

In Switzerland, the government issued a report on cryptocurrencies on 25 June 2014 stating that a virtual currency constitutes a financial asset so that criminal acts related to cryptocurrencies may constitute an offence against property as set out in Art. 137 et seq. Swiss Criminal Code, such as misappropriation (Art. 138 SCC), fraud (Art. 146 SCC), or unlawful use

11 See Art. 5 and Art. 31 et seq. of the Financial Market Supervision Act (FINMA Act).

12 Swiss Supreme Court decision 2C_119/, 9 May 2013.

13 SEC press release, SEC Emergency Action Halts ICO Scam, https://www.sec.gov/news/press-release/2017-219.

of financial assets (Art. 141bis SCC)[14].

In our view, a pump and dump scheme in the frame of an ICO should fall into the ambit of criminal fraud as defined by Art.146 of the SCC which provides: "Any person who with a view to securing an unlawful gain for himself or another willfully induces an erroneous belief in another person by misleading assertions or concealment of the truth, or willfully reinforces an erroneous belief, and thus causes that person to act to the prejudice of his or another's financial interests, is liable to a custodial sentence not exceeding five years or to a monetary penalty". The Swiss Supreme Court ruled that deceiving investors by misleading positive statements to sell them worthless securities at an artificially inflated price falls under Swiss criminal law under the offence of fraud within the meaning of Art. 146 SCC[15]. The fact that the tokens may not qualify as securities is not relevant for the application of Art. 146 SCC as the wording of this provision is not limited to securities but financial assets protected by law[16]. The misleading assertions or concealment of the truth may pertain to anything, such as advertising and glorifying an ICO project, which the organizers have no real intention to implement but only aims at selling worthless tokens. By transferring bitcoins, ether or another cryptocurrency, the deceived investor acts to the prejudice of his financial interests given the fact that cryptocurrencies have a financial value and are subject to wealth and income tax in Switzerland[17]. Therefore, the offence of fraud is characterized. Furthermore, if the tokens offered through the ICO are qualified as security (e.g. when a pre-sale of tokens entitling to acquire other different tokens at a later stage is planned[18]), the criminal provisions set forth in Art. 154 and 155 of the Financial Market Infrastructure Act (FMIA) pertaining to the specific offences of exploitation of insider information and/or price manipulation apply if their conditions are met and possibly as concurrent offences with Art. 146 SCC.

This being said, ICOs, cryptocurrencies and more generally open blockchains are creating new perennial challenges for prosecution authorities regarding the possibly non-application of certain provisions of the SCC limited to chattel, the territorial scope of application of the SCC and confiscation of crime proceeds.

First, the chapter of the SCC concerning offences against property refers to different legal concepts to delimit the application of its provisions for protecting property, such as chattel, financial assets, data, energy, etc. The SCC codifies the no penalty principle without a law (nullum crimen, nulla poena sine lege), i.e. no one may be punished for an act unless it has been

14 Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates of 25 June 2014.

15 Swiss Supreme Court decision 1A.221/2000, 20 November 2000 (extradition case).

16 Swiss Supreme Court decision ATF 117 IV 137, 17 May 1991.

17 See https://dievolkswirtschaft.ch/fr/2017/07/gennari-08-09-2017fr/.

18 FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 16 February 2018, p. 5.

expressly declared to be an offence by the law. As there is no case law yet addressing criminal offences within the context of blockchain technology, it remains partly unclear whether certain criminal activities may not be prosecuted and sentenced. As an illustration, the Swiss government and some legal scholars consider that a bitcoin is not a chattel[19]. Consequently, a bitcoin theft would not fall within the scope of Art. 139 SCC pertaining to the criminal offence of "theft" given that only the theft of "chattel" (i.e. tangible property) is covered by the wording of this provision. A bitcoin theft would however not remain unprosecutable but most likely fall within Art. 143 SCC prohibiting unauthorized obtaining of data that is stored or transmitted electronically or in some similar manner[20]. Data is not defined in the SCC but is a different concept than that of chattel[21]. Data may be defied as information represented by letters, numbers, digits, symbols, drawings, etc. transmitted, processed or stored for later use[22]. Cryptocurrencies and tokens issued, exchanged and stored on a blockchain through the use of computers will most likely be considered as data. Both Art. 139(1) SCC and Art. 143(1) allow Swiss courts to pronounce a custodial sentence up to 5 years. However, in contrast with Art. 139(2) and (3), Art. 143 SCC does not increase penalties when there are aggravating circumstances, such as committing theft on a regular basis for financial gain or as a member of a group that has been formed for the purpose of carrying out repeated acts of robbery or theft. Art. 143 SCC was introduced in 1994 when the Swiss parliament amended the SCC to fill gaps by enacting new provisions to tackle computer crime in general (Art. 143bis SCC: unauthorized access to a data processing system, Art. 144bis SCC: damage to data, Art. 147 SCC: computer fraud). However, the development in technology since may have created certain gaps. The criminal offence of handling stolen goods (Art. 160 SCC) concerns only concealment of chattels and real estate[23]. Consequently, concealment of cryptocurrencies or tokens acquired by way of an offence against property cannot be prosecuted on the basis of Art. 160 SCC. In such a case, the criminal offence of money laundering (Art. 305bis SCC) applying to the larger concept of "financial assets" may provide a legal basis for prosecuting criminals. Art. 143 SCC aims at protecting data that the owner does not want to leave accessible to a perpetrator. When the perpetrator misuses the code of the smart contract for his own unlawful gain, Art. 143 SCC may not be applicable since he

19 Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates of 25 June 2014, p. 22; Alexandre Papaux, CR Code pénal II, Ad Art. 137, N 15.

20 See Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates of 25 June 2014, p. 11.

21 Swiss Supreme Court decision ATF 128 IV 11, 6 December 2001.

22 Federal Council, Message 1991, II, p. 951.

23 Marc Henzelin/Maryam Massrouri, CR Code pénal II, Ad Art. 160, N. 16-17. The Swiss Supreme Court held in 1955 that a credit of scriptural money on a bank account is not within the scope of the definition of "goods"; economic considerations do no justify to extent the application of Art. 160 SCC [formerly Art. 144 SCC] to financial assets as such an interpretation infringes the principle no penalty without a law (see ATF 81 IV 156 = JdT 1956 IV 38).

legitimately has access to the smart contract[24].

Although the SCC will undoubtedly allow prosecution authorities to investigate ICOs and blockchain related activities, it remains to be seen whether the SCC should be revised to improve the protection of society and individuals in the context of the development of cryptocurrencies and blockchains that was not expected in 1994 when the legislator passed the bill enacting Art. 143, 143bis, 144bis, and 147 SCC to tackle computer crime.

Second, the use of a blockchain has an impact on the problem of locating the offence and identifying the criminals. There is no location for an open blockchain. The nodes, containing the blockchain, are distributed around the world. Swiss law enshrines the principle of territoriality in Art. 3 SCC, supplemented by Art. 8 SCC.

Art. 8 SCC provides that the offence is considered to be committed at the place where the person concerned commits it or at the place where the result of the offence has taken effect. The current trend is to extend the criminal jurisdiction of Swiss courts. In case of uncertainty, case law decides in favour of the competence of the Swiss authorities by application of the maxim in dubio pro duriore, in order to avoid that criminal offences being prosecuted nowhere[25]. Individuals may launch an ICO from any location as long as they have access to the Internet and sophisticated coding skills. The identification of this location and their identity may prove to be extremely difficult, in particular when the ICO was set up from the start exclusively for a criminal purpose and that the ICO organizers conceal and lies about their identity. This being said, Swiss courts may accept jurisdiction if they deem that there is a sufficient nexus with Switzerland[26]. In our view, this may be the case for instance when the ICO organizers acted in the Swiss territory, a blockchain technology start-up company related to the fraudulent ICO has been incorporated in Switzerland, organizers cash the proceeds by converting the cryptocurrencies raised into fiat money on an exchange located in Switzerland, or wire said cash to a bank account opened in a Swiss bank. Furthermore, it may be argued that the competence of Swiss prosecution authority also exists – if among the deceived investors one is a Swiss national – on the basis of Art. 7(1) and (2) SCC providing Swiss jurisdiction in particular when the place of commission is not subject to criminal law jurisdiction, by considering that the transactions taking place in the blockchain exist only in cyberspace.

Another challenge for prosecution authorities is to confiscate crime proceeds. When the cryptocurrencies have been converted into fiat

24 Pascal de Preux/Daniel Trajilovic, Blockchain et lutte contre le blanchiment d'argent, in Expert Focus 1-2/18, p. 68.

25 Katia Villard, La compétence territoriales du juge pénale suisse (art. 3 et 8 CP) : réflexions autour d'évolutions récentes, in RPS 135/2017, p. 146.

26 Ibidem.

money deposited on a bank account the usual procedure applies, and the concerned bank account will be blocked. The situation is more challenging when the crime proceeds consist in cryptocurrencies which do not physically exist. Cryptocurrencies are typically kept in a digital wallet the content of which is only accessible by the person in possession of the private key. Consequently, the possibility for prosecution authorities to confiscate cryptocurrency depends in particular on the platform providing the online wallet service and its commitment to abide by the orders from state authorities.

Criminal prosecution in the context of blockchain faces challenges due to the anonymity and decentralization. However, criminal law applies, and prosecution authorities are not completely powerless. The individuals organizing fraudulent ICOs are not exempt from prosecution.

CIVIL ACTION

Pursuant to Art. 11 Swiss Code of Obligations ("CO"), the validity of agreements is not legally subject to any form requirement under Swiss law, unless a particular form is prescribed by law (such as for assignment of claim[27]). Consequently, the participation in an ICO by an investor – who transmits cryptocurrencies to a smart contract in exchange of tokens – constitutes a valid agreement. The qualification of this agreement primarily depends upon its terms and conditions (if any) and the type of tokens at stake. Many ICOs pretend to issue utility tokens. FINMA defines them as tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure[28]. The exchange of cryptocurrencies against token represents a barter contract (Art. 237 et seq. CO) and the provision of services a mandate contract (Art. 394 et seq. CO) . It is expected that a line of defence will consist in arguing that the investor made a "donation" to the relevant foundation incorporated by the ICO organizers. Even if such a qualification would be retained, it is worth stressing that Art. 249 CO provides a right of claim for return of gift in certain circumstances such as when the recipient committed a serious criminal offence towards the donator or failed without good cause to fulfil the provisos attached to the gift.

Under Swiss law, contractual liability is subject to four cumulative conditions which are (i) a breach of contract (ii) a fault, (iii) a damage, and (iv) a causal link between the damage and the breach of contract (Art. 97 CO). The claimant bears the burden of proving the existence of the conditions (i), (iii) and (iv). The fault (ii) is presumed if the debtor has guaranteed a result. In such a case, the debtor must prove that the result could not be reached

27 Art. 165(1) CO.

28 FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 16 February 2018.

due to an event which cannot be attributed to his/her negligence (e.g. the performance becomes impossible due to force majeure). Nevertheless, for the obligations of means, the presumption of fault does not apply. Any breach of contract constitutes in fact a violation of the duty of diligence and thus a fault[29].

Depending on the structure of each individual ICO and the contractual terms stipulated (if any), different types of breaches may occur in relation to the development of a digital platform, software, or other projects which the token should allow the use and investors may be entitled to claim damages as in the frame of any non-blockchain related contractual relationship.

As for criminal proceedings, the main issue is to determine the competent jurisdiction as the traditional jurisdictional principles have limited applicability in the context of the blockchain. If there are ICO terms and conditions, the ICO organizers may have included an arbitration clause or choice of court. Otherwise, the court of the defendant's domicile or the place where the characteristic performance must be rendered (Art. 31 of the Swiss Code of Civil Procedure; Art. 112 and 113 of the Federal Act on Private International Law) is in principle competent. Where tokens are created and disseminated using distributed ledger, the concept of the place of the characteristic performance becomes rather irrelevant or has the effect of conferring jurisdiction to many states where a node would be located. The defendant's domicile is less problematic. If the ICO organizers have incorporated a company in Switzerland to launch their ICO, Swiss courts are competent (provided that it can be argued that the agreement is binding the investor to this company). In the event that the ICO organizers have not incorporated any company but used a decentralized autonomous organization (DAO), i.e. a digital company existing only on the blockchain, Swiss courts would be competent if one of the organizers resides in Switzerland. Indeed, DAO are not recognised by Swiss law as a valid type of company. As a result, the rules relating to the "simple partnership" would apply (Art. 530 et seq. CO). The launch of an ICO falls within the ambit of the definition of a "simple partnership" which is a contractual relationship in which two or more persons agree to combine their efforts or resources in order to achieve a common goal and when it does not fulfil the distinctive criteria of any of the other types of partnership codified in the CO (Art. 530 CO). The Swiss domicile of one partner establishes the jurisdiction of Swiss courts for actions directed against all partners, even if some of them are domiciled abroad (Art. 10 and 15 of the Swiss Code of Civil Procedure). Finally, an action could be brought by a Swiss investor before Swiss courts even if no ICO organizer has a domicile in Switzerland, subject to the qualification of the contractual relationship as a consumer contracts (Art. 32 of the Swiss Code of Civil Procedure and Art. 114 of the Federal Act on Private International Law).

29 Pierre Tercier, Le droit des obligations, Genève – Zurich – Bâle 2012, p. 268 f., N 1197.

Foreign investors could join this action on the basis of Art. 15 (2) of the Swiss Code of Civil Procedure, which provides that where two or more actions that are factually connected are raised against one and the same defendant, each court that has jurisdiction over any one of the actions has jurisdiction over all of them.

CONCLUSION

In a fast-changing world, ICOs offer an attractive target for savvy criminals and ICO organizers may have the feeling that investors have no contractual duty towards investors. Investor claims require a multidisciplinary approach to enhance the chances of success of legal action. Depending on the circumstances, an investor who has been defrauded may access the criminal file and use this information in a future claim for damages before civil courts. Swiss law also provides for filing a civil claim for damages within the criminal proceedings. Although a deceived investor has no right of party in FINMA enforcement proceedings, FINMA and the prosecution authorities shall exchange the information that they require in the context of their collaboration and in order to accomplish their duties. FINMA's investigation report may therefore be obtained through criminal proceedings. In 2018, ICOs and cryptocurrencies are highly likely to be more regulated by states exercising their power to restore law and their control in these areas, increasing volatility. Deceived investors having lost substantial amounts will certainly initiate legal action and case law will emerge in this fascinating new area.