PAYSYS REPORT

Issue 07 November 2016

In this issue:

5AMLD: The end of anonymous online payments

(hg) As a consequence of the terrorist attacks in Paris, the European Commission prepared an Action Plan to intensify the fight against the financing of terrorism. The rough intentions of the Action Plan were published on 2 February 2016. The March terrorist attacks in Brussels seemed to confirm the Commission to be on the right track. On 5 July 2016 the Commission proposed a first concrete step by tightening the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("4AMLD"), which was agreed in May 2015 and which should be implemented by the Member States by the latest in June 2017. Yet the proposal for the new AML-Directive ("5AMLD") is supposed to be implemented in a cloak-and-dagger operation within a few months by targeting an effective start date of 1 January 2017 (!). By re-opening the 4AMLD, the Commission has created a quite unique legislative procedure to implement an amendment of an adopted Directive before its full implementation. The specific areas of amendments are:

- Enhanced due diligence measures/counter-measures with regard to high-risk third countries,
- Virtual currency exchange platforms,
- Prepaid instruments,
- The access of Financial Intelligence Units (FIUs) to – and exchange of – information (to strengthen FIU powers and co-operation),
- The access of FIUs to centralised bank and payment account registers or electronic data retrieval systems.

These targeted areas, which will not be discussed here in detail, are not only related to the terrorist threat, but also to unveiled risks of tax evasion and money laundering as a consequence of the recent publication of the so-called "Panama Papers". Prepaid cards are on the agenda of the Action Plan because these payment instruments, probably issued anonymously, are actually used ("misused") by terrorists in Paris and Brussels for preparing their attacks. There is no evidence for the usage of virtual currencies by terrorists, but these instruments should be included as a preventive measure.

Our Comment:

The Commission launched the proposal for the 5AMLD on July 5th. The very next day, the report of the inquiry into the UK involvement in the Iraq War of 2003 was published, after an investigation lasting almost 7 years, by a committee of inquiry chaired by Sir John Chilcot. The Chilcot Report analysed inter alia the role of intelligence in misleading the UK government through questionable reports of alleged weapons of mass destruction in possession of the Iraq army, which was the decisive reason for starting the Iraq War by the USA and UK. Most of us remember the slides publicly presented in 2003 by the US Administration showing imaginary trucks with hidden chemical, biological or even nuclear weapons. However, during the war the US troops failed to find these weapons of mass destruction. The day after the publication of the Chilcot Report, the former UK Prime Minister Tony Blair apologized for being so naive as to believe the "facts" presented by intelligence. That was the end of the matter. The Chilcot Report disappeared into the summer 'silly season' 2016. It is tedious to discuss the reasons behind the misleading information provided by British and American intelligence. Fact is, information can be wrong and at the very least the information should be interrogated for its relevance. We have to keep this in mind when analysing the proposal for the 5AMLD regarding prepaid cards, which is also based on "facts" provided by intelligence.

Despite its far reaching consequences for privacy and human rights in digital space, the Commission´s proposal has not yet come to public attention. Maybe it was also just part of the summer 'silly season'. However, it is worth taking a closer look.

Virtual currencies

Terrorists could benefit from virtual currencies (e.g. Bitcoin) or e-money (like prepaid cards) because both instruments could be used anonymously by their users, although every transaction is tracked and digitally stored in contrast to cash which leaves no digital fingerprints at all. At the physical Point-of-Sale terrorists prefer cash if they don´t want to leave traces (by the way: someone might doubt the relevance of anonymity for the currently dominant new kamikaze-type of terrorist). The prohibition of cash would be the only effective measure to prevent anonymous transactions by terrorists in this market segment. This could be a long-term target, but it is not part of the recent Action Plan of the Commission for short-term actions in its fight against terrorism.

For internet transactions, most of the online means of payment are related to payment instruments, which are issued to their users and subject to full KYC requirements (Know-Your-Customer by identification and verification), like debit and credit cards, e-money accounts (like PayPal) or bank account related instruments (like iDEAL or Sofort). Bitcoin and most of the other virtual currencies are a thorn in the eye of regulators because they lack the role of an issuing and acquiring instance in their eco-system, which are usually subject to regulation and are the addressees of KYC requirements. For the time being, the only way to get regulatory control of these systems is the regulation of the tangible exchange platforms, which should now be subject to the KYC user requirements according to the 5AMLD.

However, virtual currencies are still not generally accepted for online payments and ecommerce. The 5AMLD is a relatively symbolic and harmless action with potential preventive effects without hurting the financial transactions of terrorists and without perceptible impacts on the legal payment markets, where transactions with virtual currencies currently play no role. Its relevance is its political message to frightened citizens wanting action from politicians to fight terrorism. Most of the players in the virtual currency market could even welcome this measure as a sign from the regulators of legitimizing these private currencies. This remarkable unwanted side-effect of the 5AMLD has already been criticized by the ECB in its recent statement[1].

Lowering thresholds

However, the impact of the 5AMLD on the European e-money market has more relevance. Most of the payment instruments that are linked to e-money (card- or account-based) are usually issued by applying Customer Due Diligence (standard or simplified CDD). According to the Third Anti-Money-Laundering Directive (3AMLD of 2005), Member States could exempt the CDD requirements for low-risk e-money. These products should be limited regarding usage and storage of the funds, which could differ for reloadable and non- reloadable instruments (see table). Almost all Member States have integrated this option for anonymous e-money into national laws.

E-Money Instrument⇩ / EU-Directive⇨	3AMLD Status Quo 2016	4AMLD Transposition June 2017	5AMLD Proposal Commission
not reloadable			
max. stored value			
* domestic & cross-border usage	250 €	250 €	150 €
* only domestic usage	500 €	500 €	150 €
reloadable			
max. transaction volume per calendar year			
* per calendar year	2.500 €		
* per month	no limit	250 €	150 €
max. amount for redemption per calendar year	999.99€	no limit	no limit
max. stored value	no	500 €	150 €
limited to domestic usage only	no	yes	yes
not reloadable & reloadable			
max. redemption in cash		100 €	50 €
usage limited to purchase goods & services	no	yes	yes
usage limited to face-to-face transactions	no	no	yes
funding with anonymous e-money	yes	no	no

After a long legislative process the 4AMLD was adopted in May 2015. With regard to potential (not current) risks of anonymous e-money for money-laundering and terrorism financing, the thresholds for usage of reloadable payment instruments have been considerably reduced. The new requirement of a strongly limited cash redemption (100 Euros) makes these prepaid products hardly suitable for money laundering. Furthermore, the instrument can only be used in the country of issuance for purchasing goods and services (no P2P money transfer).

No Member State has yet implemented the 4AMLD. Therefore, no one has any idea how effective these measures are in achieving their aims. However, the Commission claims in its Proposal for the 5AMLD, the restrictions of the adopted 4AMLD are "*insufficient*" or *"have been identified as ineffective or only very marginally effective to reach the general and specific objectives"*[2]. The Commission published an extended Impact Assessment (IA), but without any facts which could justify this claim. In consequence, the insufficiency and ineffectiveness of the agreed, but not yet implemented restrictions on e-money of the 4AMLD is an unproven hypothesis. Someone could claim the opposite, that the 4AMLD is sufficient. Both claims are equally valueless hypotheses.

Besides the lowering of the thresholds, the Proposal includes two other critical issues for prepaid instruments:

Issuing

If the prepaid instrument is used for online payments[3] the CDD exemption is invalid. As a consequence of the CDD exemption for e-money, the usage of a prepaid instrument is today the last remaining possibility for anonymous consumer payment transactions on the internet within the existing thresholds, which mitigate the risk of AML and terrorist financing. For e-commerce with physical goods anonymity is probably less important for the necessary delivery of purchases to a buyer address.

The insufficiency and ineffectiveness of the agreed, but not yet implemented restrictions on e-money of the 4AMLD is an unproven hypothesis.

Someone could claim the opposite, that the 4AMLD is sufficient. Both claims are equally valueless hypotheses.

For digital services and goods (like paid access to digital content) anonymity of the user is still a human right, even in the digital world of today where users are happy to give their personal data willingly in exchange for free digital services (Google, Facebook etc.). The end of anonymous internet payments would be rather a contradiction to the new business model proposed by privacy supervisors, where service providers like Google and Facebook should offer the option of paid services for users who don´t like to exchange their personal data for free services. The logical consequence of this business model should be the option of an anonymous payment.

In its IA, the Commission recognizes in principle "*the need to protect fundamental rights, including data protection, and economic freedoms*"[4].

"*Any measure limiting currently existing anonymity will have direct effect restricting privacy and data protection. The more effective the measure is with respect to lifting anonymity, the greater the impact on privacy and data protection rights of users of the cards. The options with least negative impact on data protection are the least effective to attain the objectives pursued.*"[5]

However, it is striking that the Commission rates the proposed measure of the termination of anonymous payments with e-money for internet payments with "zero" (no impact) in the comparison to status quo in its IA.

What is the opinion of the European Data Protection Supervisor (EDPS)? The Commission consulted the EDPS at a very early stage (April 2016). The preliminary EDPS comments were not published. However, there was no mention of a ban on online payments at this time. The EDPS is still silent on the 5AMLD-Proposal.

Acquiring:

According to the Commission´s Proposal, acquirers are not allowed to accept prepaid cards issued in countries outside the EU where such cards do not meet the requirements equivalent to those of the 5AMLD. This equivalence requirement is not practicable because an acquirer has no knowledge of the restrictive product features of the prepaid cards (thresholds) which are accepted by its merchants. The acquirer cannot even technically recognize the product feature "prepaid" (issued as e-money) from the majority of cards issued outside the EU. To comply with this requirement, the acquirer and its contract partners (merchants) have to refuse all cards from outside the EU, which is a truly nightmare scenario for European card business.

NB: This requirement is restricted to prepaid cards only, whereas the restrictions on the issuing side are applicable to all e-money products, which is not consistent from a systematic legal point of view.

The focus of the Commission is de jure the prepaid instrument market (all e-money products), de facto it wants to target the **general purpose prepaid cards**, supposedly used by terrorists. These prepaid "credit" cards are in Europe mainly issued by licensees of the international card schemes Mastercard and Visa. The Commission claims erroneously that the prepaid instrument market is essentially a prepaid card market[6], which could explain the slip of bringing different products into the regulation on the issuing and the acquiring side of the market in the same article (12) of the Proposal. According to ECB statistics only 22% of the e-money transaction volume was generated by cards in 2014.

Facts

One or more terrorists used an anonymous reloadable prepaid card, branded by Visa or Mastercard, issued in one of the Member States in preparing the attack of November 2015 in Paris. It was – according to the case study by the Commission[7] - used for car rental and for booking flats and/or hotels. The card was topped up several times in excess of 750 Euro in total. These are all the facts, probably from intelligence sources, that we have to deal with. The Commission is at the time being not willing to or cannot deliver more information.

Several questions remain unanswered. Could the attacks have been prevented if the terrorists had used non-anonymous credit cards? What would be the real advantages for the search for traces of an accomplice in this case? Would the terrorists not have to identify themselves for hotel accommodation and car rental anyway? The Commission, on the other hand, reports a clear advantage over the use of anonymous cards against cash: It was precisely through the use of the card (unlike cash) that it was possible to trace in retrospect the purchase activities and locations of the terrorists. Furthermore, this case shows the effectiveness of the thresholds of the 4AMLD (250€ limit per month) to make the preparations of terrorists more complicated.

The Commission admits that the proposed measures have to be considered more as a prevention. In the IA, the Commission does not provide any arguments for the termination of anonymous **online** payments. The cards were obviously used for online reservations (car/hotel), the payments for these services could also still be made in cash. The question remains: Why online payments? The Commission answers this question only indirectly: The best way to fight terrorism would be the termination of all anonymous payments. Because cash still exists, this measure would not be effective for payments at the physical POS. In the digital world, however, there is no such alternative except anonymous prepaid cards. This simple answer does not lack logic.

Other Reasons

A more hidden argument of the Commission to further minimize the usage of anonymous prepaid instruments according to the IA is to highlight the missing level playing field between low-risk prepaid cards, which could be issued anonymously and bank-issued card products like debit and credit cards, which are subject to full KYC. The prepaid card industry would have an unjustified advantage compared to the banking industry. This is hardly convincing, because the low-risk anonymity is a feature related to the product "e-money", which can be issued by all players, banks and e-money institutions in exactly the same way.

Market of anonymous payments

The IA quantifies the yearly payment volume generated anonymously by prepaid cards on some pages to € 11 billion p.a., elsewhere to € 5.4 billion p.a. These volumes are generated by approx. 2.1 million anonymous prepaid cards (reloadable and non-reloadable). A quick plausibility check gives an absurd result of a sales volume per card of € 2,571 to € 5,238 Euro, whereas the maximal limit per card is legally fixed at € 2,500 Euro per reloadable card by the 3AMLD. If we take into account the 88% share of non-reloadable cards, as assumed by the Commission, the expenditure per reloadable card would be about 41,000 Euro (!) per card, which is not credible.

Both results are fundamentally wrong! This eliminates the relevance of all cost estimates of the proposed measures of the Impact Assessment.

The results (€ 5.4 billion or € 11 billion) are not only contradictory, but are based on a misinterpretation of existing data on the e-money market, delivered by the ECB and the Electronic Money Association (EMA). Both results are fundamentally wrong! This eliminates the relevance of all cost estimates of the proposed measures of the IA.

In its IA the Commission disregards other non-card-based e-money products, which are subject to the regulations. As a consequence of the PSD2, the exemption for payment instruments in the so-called **limit networks** (Art. 3 k) will be further restricted as an explicitly stated target of the PSD2. Prepaid products like multi-merchant gift cards and loyalty schemes are particularly affected. Already today, Esprit and Lidl gift cards are issued as e-money and therefore subject to regulation. At the end of the day, full KYC for multi-merchant gift cards, which can be used for internet shopping, would be the bizarre outcome of the well-meaning actionism of our brave terrorism fighters in Brussels.

Current Status

Where do we stand today? Although the legislative process is well advanced, the targeted implementation date of 1 January 2017 has been postponed to 6 months after publication (Q4 2017 as probable date for implementation) at the latest (no synchronicity with the 4AMLD).

On the acquiring side the "equivalence" requirement does not have to be realised by the acquirer anymore. Member States shall ensure that **payment card schemes** (instead of acquirers) have to prevent anonymous prepaid card payments by issuers outside the EU with non-equivalent thresholds. The relevant payment card schemes are located outside the EU. How should a single Member State ensure this? The Council adds in its latest Presidency compromise text (25 November 2016): "*Member States may decide not to accept on their territory payments carried out by the anonymous prepaid cards*". Again an unconscious requirement. If e.g. Germany made this decision, how should an acquirer located in Germany block all the anonymous prepaid cards issued in other Member States? How could Germany prevent the acceptance of these cards, if the acquirer of the German merchant is located outside Germany?

The good news: On 7 November the leading committees of the EP kicked out the CDD requirement for online payments. However, the latest Presidency compromise text of the European Council (25 November) still retains the online-clause which should come into force after **3 years** as "sufficient transitional period". Until this proposed definitive termination, online payments with anonymous prepaid instruments were allowed for amounts below €50. The amended text now includes all "remote" payments, therefore extending the requirement to contactless payments with prepaid instruments at the physical POS. By postponing the implementation date of the online/remote clause by 3 years, the Council obviously doesn´t support the great urgency of the Commission´s proposal regarding the suggested massive threat of terrorists using prepaid cards for internet shopping. However, the Council insists on an unjustified necessity of implementation in 3 years (probably 2020). Why not just wait for the effects of the measures of the 4AMLD with its new strong limitations for prepaid instruments?

The 4AMLD has to be implemented in 2017 at the latest. Between then and 2020 there is enough time to collect really hard facts regarding the assumed "misuse" of anonymous prepaid instruments, which cannot be supplied today by the Commission. It makes no sense to take a decision in advance *without* facts with relevance in 3 years, if you could make the same decision in 3 years *with* facts. Regarding the huge impact on privacy and human rights, we should use this period for a public debate about the pros and cons of the termination of anonymous internet payments. At the same time, the Commission could improve its poor IA[8] and terrorists would have enough time to relaunch their cash-strategy.

Remember the statement of Sir John Chilcot during the presentation of his Iraq Inquiry: "*It is now clear that policy on Iraq was made on the basis of flawed intelligence and assessments. They were not challenged, and they should have been.*"[9]

Notes

1. See Opinion of the European Central Bank of 12 October 2016: https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf
2. IA, p. 63
3. There is no clarity in the Proposal what exactly online payments means: remote payments, card-not-present-payments, e-commerce-transactions?
4. IA, p.11
5. IA, p. 63
6. IA p. 157
7. IA, p. 8
8. Regarding the quality of the IA see also the briefing „Prevention of the use of the financial system for the purposes of money laundering or terrorist financing" of the EPRS (European Parliamentary Research Service) of October 2016. http://www.statewatch.org/news/2016/nov/ep-briefing-money-laundering-terrorist-financing-11-16.pdf
9. http://www.iraqinquiry.org.uk/media/247010/2016-09-06-sir-john-chilcots-public-statement.pdf

Should you have any questions or comments please contact:

Dr. Hugo Godschalk (hgodschalk@paysys.de)
Dr. Malte Krueger (mkrueger@paysys.de)

Please, send us your views to:
paysys-report@paysys.de

PAYSYS REPORT IMPRINT

PaySys Consultancy GmbH
Im Uhrig 7
60433 Frankfurt /Germany
Tel.: +49 (0) 69 / 95 11 77 0
Fax.: +49 (0) 69 / 52 10 90
email: info@paysys.de
www.paysys.de

PAYSYS REPORT
November 2016

Layout: cristina dresler | kommunikation+gestaltung

Subscription info:
The PAYSYS REPORT is published 10 times a year in English in electronic format (pdf) and contains about 4-6 pages.
The price is
250 EUR per year (single user license)
500 EUR per year (company license)

To order, please send an email to paysysreport@paysys.de indicating the type of license you wish to purchase and the method of payments (credit transfer or credit card).

PaySys Consultancy is German member of

epca european payments consulting association