EUROPEAN COMMISSION

Brussels, 19.4.2018
C(2018) 1649 final

Dear President,

The Commission would like to thank the Bundesrat for its Opinion on the Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA {COM(2017) 489 final}.

This proposal was adopted as a part of the package of measures presented on 13 September 2017 and designed to enhance cybersecurity in the European Union.

In proposing this initiative, the Commission is following up on the commitment it undertook in the European Agenda on Security {COM(2015) 185 final} to review the existing European Union legal framework, which dates back to 2001, and remedy identified shortcomings.

The European Union has already put a number of instruments in place to enhance online payments security. Moreover, Member States have included non-cash payment fraud among the priorities for law enforcement cooperation within the EU policy cycle. Europol's European Cybercrime Centre has in the recent past supported and contributed to several successful operations.

Technological developments have brought about substantial changes in the area of non-cash payments and fraud is increasingly moving online. As a result, the criminal law framework needs to evolve as well, to make sure that crimes can be effectively prosecuted, also when offences are committed with newer payment instruments. The same is true for preparatory acts for non-cash payment fraud, such as stealing and selling security credentials.

To address the identified gaps, the proposal for a new Directive on combating fraud and counterfeiting of non-cash means of payment aims to:

1) *Update the legal framework to make sure that crimes can be effectively prosecuted, also when offences are committed with newer payment instruments, while they are currently criminalised differently in Member States or not criminalised.*

Mr Michael MÜLLER
President of the Bundesrat
Leipziger Straße 3 - 4
D – 10117 BERLIN

2) *Remove operational obstacles to reduce the time needed to provide information in cross-border cooperation and enhance investigation and prosecution of crime and increase reporting of crime to law enforcement authorities.*

3) *Enhance prevention and assistance to victims and support public-private cooperation to effectively fight and prevent crime – which still suffers from gaps in information sharing – and avoid that criminals exploit the lack of awareness of victims.*

In response to the more technical comments in the Opinion, the Commission would like to refer to the attached annex.

The Commission hopes that the clarifications provided in this reply address the issues raised by the Bundesrat and looks forward to continuing the political dialogue in the future.

Yours faithfully,

Frans Timmermans
First Vice-President

Dimitris Avramopoulos
Member of the Commission

ANNEX

The Commission has carefully considered each of the issues raised by the Bundesrat in its Opinion and can offer the following clarifications.

1. *The Commission agrees with the Bundesrat that the approximation of criminal laws and regulations of the Member States through European Union criminal law should be proportionate and should prove essential to ensuring the effective implementation of the Union policy in this field. The extent to which the proposal fits the principles of subsidiarity and proportionality was carefully analysed and considered in the impact assessment study and in the actual drafting of the proposal.*

2. *The declared aim of the proposal is to ensure that the criminal law framework is technology neutral. Given the fast technological evolution of payment systems, the Commission sees this as the only way for it to be truly future-proof. This would be achieved only if at least all known means of payment are covered, including virtual currencies, which have reached an unprecedented market value*[1]*. The fact that criminals abuse the anonymity that some virtual currencies provide in order to avoid detection, as they do with several other technologies, should not be a reason to deny the protection provided by criminal law to many legitimate users.*

3. *The threat assessments produced at European Union level over recent years*[2] *consistently show how the 'crime-as-a-service' business model, where criminals sell and buy online the illegal services and tools they need, lowers the level of capacities needed to engage in cybercriminal activities and provides for the possibility to divide roles within criminal networks. For this reason, the Commission believes that conducts that are preparatory to fraud should be criminalised as self-standing offences. These behaviours (for instance, the sale, transport, or mere possession of stolen or counterfeited payment instruments) are harmful per se and represent a violation of privacy.*

4. *The fact that fraud often takes place online challenges the traditional concept of territoriality because information systems can be used and controlled remotely from anywhere. Therefore, competent authorities should assert their jurisdiction over offences where the perpetrator is a national of their country or is physically present in the territory of their Member State. Moreover, with a view to ensuring that appropriate law enforcement and judicial action can be taken in the country where it is most likely for victims to report the offence, jurisdiction should also be asserted on the grounds of the territory where the damage caused by the offence occurs.*

---

1 As of 5 December 2017, the market value of the main virtual currencies is around USD 200 billion (see https://blockchain.info/charts/market-cap).

2 For instance: 2017 Internet Organised Crime Threat Assessment (IOCTA – available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017) and European Union Serious and Organised Crime Threat Assessment 2017 (SOCTA – available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017)

5. *The impact assessment carried out by the Commission in preparation of the proposal showed an acute lack of data concerning these crimes, which makes it difficult to combat them effectively. The Commission is aware that the collection of statistics represents an additional burden on national administrations. This burden was estimated in the impact assessment, based on a minimum number of indicators and statistical data. Without a minimum of statistical data, it is difficult to evaluate the effectiveness of the tools used to combat these crimes.*