Combating fraud and counterfeiting of non-cash means of payment

2017/0226(COD) - 13/09/2017 - Legislative proposal

PURPOSE: to effectively combat fraud and counterfeiting of non-cash means of payment.

PROPOSED ACT: Directive of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: fraud and counterfeiting of non-cash means of payment (including payment cards) is a threat to security:

- as it **represents a source of income for organised crime** and is therefore an enabler for other criminal activities such as terrorism, drug trafficking and trafficking in human beings;
- as it is also an **obstacle to the digital single market**. In 2013, fraud using cards issued in the Single European Payment Area (SEPA) reached EUR 1.44 billion, representing growth of 8% on the previous year. 42% of users are concerned about the security of online payments.

The European Agenda on Security acknowledges that Framework Decision 2001/413/JHA insufficiently addresses new challenges and technological developments such as virtual currencies and mobile payments.

Currently:

- **certain crimes cannot be prosecuted effectively** because offences committed with certain payment instruments (in particular non-corporeal) are criminalised differently in Member States or not criminalised;
- too much **time** is taken to provide information in cross-border cooperation requests, hampering investigation and prosecution;
- **information sharing gaps** in public-private cooperation hamper prevention and criminals exploit the lack of awareness of victims.

Framework Decision 2001/413/JHA therefore needs to be **updated and complemented** by new provisions on offences, penalties and cross-border cooperation.

This proposal has **three specific objectives** that address the problems identified:

- ensure that a clear, robust and technology neutral policy/legal framework is in place;
- eliminate operational obstacles that hamper investigation and prosecution;
- enhance prevention.

Furthermore, revising the present rules will **enhance cooperation between the police and judicial authorities** as well as between law enforcement agencies and private entities and will contribute to achieving the objectives of the 2001 Council of Europe **Cybercrime Convention** (Budapest Convention), which represents the international legal reference framework for the EU.

IMPACT ASSESSMENT: since the problem is essentially due to a **regulatory loophole**, the preferred option is to introduce a new legislative framework and to facilitate self-regulation for public-private

cooperation and encourage reporting for public-private cooperation instead of self-regulation, and new provisions on raising awareness.

CONTENT: the proposal for a Directive seeks to establish **minimum rules concerning the definition of criminal offences and sanctions in the area of fraud and counterfeiting of non-cash means of payment**. While abrogating Framework Decision 2001/413/JHA, the proposal updates most of its current provisions.

Specifically, this proposal:

- **defines payment instruments in a broader way**, including also 'digital exchange instruments', i.e. any electronic money within the meaning of Directive 2009/110/EC of the European Parliament and of the Council, and virtual currencies;
- **criminalises** not only the fraudulent use of payment instruments by means of stolen or falsified payment authenticators but also the possession, sale, obtaining for use, importing, distribution or any other form of making a false or falsified, stolen or appropriate payment instrument available by other illegal means. It covers all offences involving payment instruments, whether they are corporeal or not, and therefore also applies to behaviour such as trade in stolen credentials (‘carding’) and phishing;
- criminalises acts such as **hacking a victim’s computer or a device** in order to re-direct the victim’s traffic to a forged online banking website, thus causing the victim to make a payment to a bank account controlled by the offender;
- **introduces rules on the level of penalties**: it sets a minimum level for maximum penalties (at least three years imprisonment) and provides for more severe penalties (at least five years imprisonment) for aggravated offences, namely: (i) situations where criminal acts are committed within the framework of a criminal organisation; (ii) situations where crime is conducted on a large scale causing considerable overall harm or where a crime involves an aggregate advantage for the offender of at least EUR 20 000;
- clarifies the **scope of the jurisdiction** regarding the offences referred to in the proposal by ensuring that Member States have jurisdiction in situations where the offender and the information system that the offender uses to commit the crime are located in different territories;
- obliges Member States to ensure that **victims of non-cash payment fraud** are offered information and channels to report a crime and advice on how to protect themselves;
- introduces measures to **improve Union-wide criminal justice cooperation** by strengthening the existing structure and use of the operational contact points;
- stresses the need to **raise awareness** and thus reduce the risk of becoming a victim of fraud by means of information and awareness-raising campaigns, and research and education programmes.

The Commission shall assess the effects of the Directive six years after the deadline for its implementation.