EUROPOL

Public Version

Situation Report

Payment Card Fraud in the European Union

Perspective of Law Enforcement Agencies

This Europol product analyses and evaluates the threat posed by types of serious or organised crime. The assessment of threats is based on defined indicators.

Images: Fotolia

Table of Contents

Europol would like to thank its cooperation partners for their support in producing this report: EU law enforcement authorities; American Express; MasterCard; Visa Europe; EAST (European ATM Security Team); ECB (European Central Bank); EPC (European Payments Council).

1. KEY JUDGMENTS

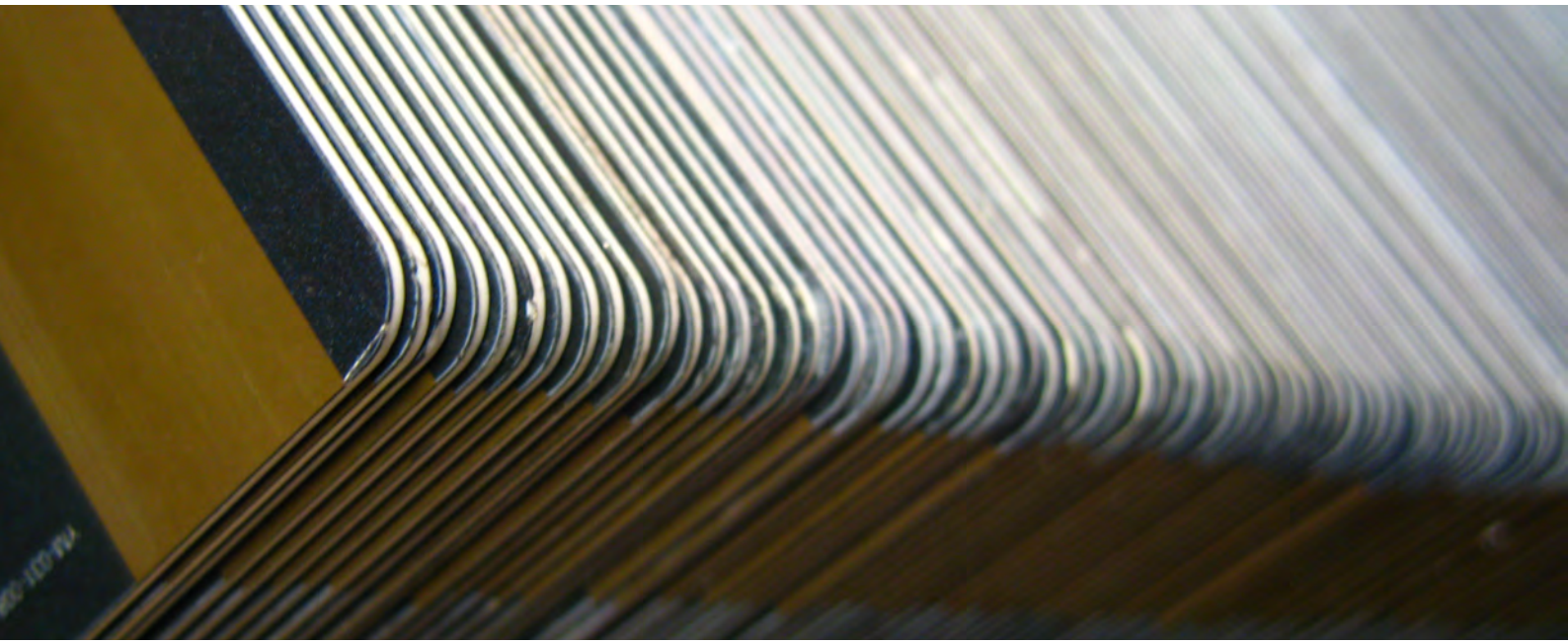
- The criminal market of payment card fraud (PCF) within the European Union (EU) is **dominated by well structured and globally active organised crime groups (OCGs).** Criminal networks have managed to affect non-cash payments in the EU to the extent that protection measures are very expensive and need to be implemented on a global level. Consequently, the use of payment cards can be inconvenient and no longer fully secure for EU cardholders.

- Payment card fraud is a low risk and highly profitable criminal activity which brings organised crime groups originating from the EU a yearly income of around **1.5 billion euros**. These criminal assets can be invested in further developing criminal techniques or can be used to finance other criminal activities or start legal businesses.

- The EU is increasingly exposed to the threat of illegal transactions undertaken overseas and should develop more efficient solutions to help law enforcement authorities (LEAs) combat the fraud. Europol, gathering intelligence on fraudulent overseas transactions affecting the EU, as requested by competent authorities of Member States (MS), is not entitled to cooperate with non-EU police forces or request specific measures to help combat and prevent fraud against the EU. **A special mandate for Europol** is recommended to dismantle globally-active OCGs and protect the EU against further fraud committed through non-cash means of payment.

- The majority of illegal face-to-face card transactions (skimming-related) affecting the European Union take place overseas, mainly in the United States. The EU should take urgent measures to **promote the EMV standard** as a global solution against the counterfeiting of payment cards. As full EMV implementation will take time, a temporary solution could be applied, namely the implementation of GeoBlocking – blocking overseas transactions using EU-issued cards unless they have been activated in advance.

- Common European legal solutions for the security of on-line retail payments (internet, mobile), as well as the mandatory reporting of financial data breaches, should be considered to prevent fraud affecting EU citizens. Prevention and combating card-not-present (CNP) fraud requires specific regulations on the customer's identification (3D secure protocol) and security of the on-line payment environment. The role of the European Central Bank and Europol is crucial to present the problems and propose specific solutions.



2. Introduction

2.1. Background

The security of non-cash means of payment is a key factor in the economic stability of the European Union (EU). According to statistics[1], the total number of payment cards issued in the EU in 2011 reached 726 906 710. The value of legitimate non-cash transactions with EU cards exceeded 3000 billion euros. From a security perspective, EU industry has taken an important step forward by fully implementing the EMV (chip-embedded cards) standard for card-present (CP) transactions, and is advanced with the protection of on-line transactions through the strong identification of customers (3D secure).

Banking institutions are profit-making businesses, so reducing the illegal income of criminals is not always a priority for them when introducing new banking products or services. Acceptable levels of fraud and expected net profit for banks are more important than the real prevention of fraud that would lead to depriving criminals of the huge amounts of money they are stealing using EU payment cards. With the current global nature in which the banking sector and non-cash transactions operate, security measures in place on a regional (EU) level are not sufficient and have been exploited by criminal networks.

The illicit activities and fraudulent transactions of organised crime groups (OCGs) performed outside the EU have affected the security and convenience of non-cash payments in Europe and have consequently caused substantial losses to the EU economy. European law enforcement authorities (LEAs) have collected information and intelligence on the activities and development of the OCGs responsible for payment card fraud. Europol has processed and analysed the data in order to define the most vulnerable areas and provide some recommendations.

This report is based mainly on data provided by law enforcement agencies from EU Member States and some cooperating non-EU States. The figures and latest trends were identified based on information from the European Central Bank, European Payments Council, European ATM Security Team (EAST), card schemes, Fuel Industry Card Fraud Investigation Bureau (FICFIB) and some card issuers.
Since criminals affect both physical transactions with payment cards (shops, ATMs), and the internet environment, for the purpose of this report payment card fraud (PCF) is divided into **card-present (CP) fraud** and **card-not-present (CNP) fraud.**

[1]Official statistics from the European Central Bank.

2.2. Aims and objectives

The main objective of this report is to present threats posed by criminal structures and propose specific solutions. The ultimate goal for Europol is to make non-cash payment transactions safer. According to a Europol study, the income of organised crime groups (OCGs) of European origin is fairly consistent at around 1.5 billion euros per year. These proceeds of crime are typically invested in further technical developments, used for financing other criminal activities or used to start legal businesses.

This report aims to provide detailed information on the current situation and the most important trends affecting EU transactions and payment cards. The following aspects are covered by the report:

- overview of payment card fraud in the European Union,
- structures and activities of organised crime groups affecting non-cash payments in the EU,
- possible solutions to the problems.

3. Combating Payment Card Fraud in the European Union

In 2011 Europol provided support to EU law enforcement authorities (LEAs) in hundreds of international investigations of payment card fraud (PCF). The majority of the crimes had an international dimension – taking into account the origins of suspects, places where card data was obtained and illegal transactions made, and the final destination of the criminal proceeds. The specialised team at Europol produce analytical reports and organise meetings to facilitate cooperation on combating PCF crimes.

The majority of illegal transactions took place outside the EU, but affected the EU. Despite the huge number of identified perpetrators, many of them remain unidentified and are still actively involved in payment card fraud.

A criminal structure involved in PCF is usually very complex, highly specialised and hierarchical, with specific roles assigned to each member of the OCG. Europol has coordinated several cross-border investigations against worldwide criminal networks affecting the EU.

For the purpose of this report Europol conducted a research poll among EU payment card fraud investigators about the major challenges for LEAs in this area. Experts reported that the international aspect

of criminal networks, and their highly-organised nature, as the biggest problems faced during the operational phase[2]. Criminals benefit not only from the lack of global protection standards but also from the legal constraints affecting international police cooperation. As far as the organisational approach is concerned in MS, there are different police units responsible for combating this phenomenon: economic units; forgery of money units; cybercrime units; or specialised PCF units, sometimes supported by representatives from the private sector. This is also seen as a factor that makes international cooperation more difficult due to different perceptions of the crime and its prioritisation in respective units.

Europol, which has an excellent overview on the global activities of the OCGs, has no legal or organisational possibilities to cooperate directly with most of the non-EU police authorities . Despite many attempts, neither the Interpol channel nor the legal provisions of Article 23, p.8, of the Europol Council Decision (ECD)[4] have been useful in initiating investigative measures into criminal structures active overseas. Europol, having precise intelligence and information about ongoing criminal activities against the EU, and being aware of the scale of the problem, are entitled to cooperate with non-EU States to support and coordinate investigations in EU Member States.

The main challenges in combating PCF	1-5
Cross-border crime	4.4
Well structured OCGs	3.8
Cooperation with judicial authorities	3.7
Awareness of cardholders	3.5
Cooperation with the private sector and financial institutions	3.4
Cooperation with other LEAs	3.3
Necessary knowledge among police officers	3.3
Priority of payment card fraud	3.3
Legal and organisational restrictions	3.0

Table: Results of the research poll to law enforcement agencies

[2] Ten challenges were reported by Member States and rated on a scale from 1 (no challenge) to 5 (very challenging).

[3] Europol has operational agreements with the following countries: Australia, Canada, Croatia, former Yugoslav Republic of Macedonia, Iceland, Monaco, Norway, Switzerland and the United States.

[4] Europol may transmit personal data and classified information to third countries if absolutely necessary to safeguard the essential interests of EU Member States.

With the relatively lenient laws for perpetrators and limitations for law enforcement authorities on combating payment card fraud, as well as difficulties in seizing assets, payment card fraud is very attractive and highly profitable for criminal networks. Europol analysis indicates that the same criminals are still active in this criminal market after many years and, after being arrested, they return to the business after just a few months.

4. Card-present (CP) fraud

4.1. Introduction

The implementation of EMV[5] (Chip and PIN) technology in the European Union is seen as the key driver to reducing domestic payment card fraud. It should be stressed that cardholders' confidential data is more secure on a chip-embedded payment card than on a magnetic strip card. Chip-embedded cards support dynamic authentication, requiring dynamic values for each transaction, and cannot be easily copied. The EMV card is considered to be well protected against skimming.

As the EU banking industry migrates to the EMV environment, losses caused by illegal domestic transactions in the EU have gradually decreased since 2008. However, at the same time, the level of illegal transactions overseas has seen a sharp increase. Consequently, in 2011, almost all fraudulent face-to-face transactions with EU cards took place overseas. This phenomenon is determined by the level of technical protection of EU payment card terminals - ATM and Point-of-Sale (POS) terminals are fully EMV compliant. In response, criminal networks have targeted the weak points of the system and have undertaken criminal activities using non-EMV compliant terminals overseas. Due to this phenomenon, and the lack of specific agreements on reimbursement of losses caused by less protected terminals, the majority of the loss burden caused by this fraud is on the EU card issuers – which are specific banks in the EU. It is worth mentioning that there has been no specific solution to this problem proposed by the card industry.

There are several countries operating as a substantial market for illegal transactions with counterfeit EU cards. The problem of illegal transactions in the US has been reported to Europol by all 27 EU Member States (MS). There are also other locations where criminal groups with EU origins are cashing counterfeit cards.

[5] EMV (Europay, MasterCard, Visa) - a global standard for payment cards based on chip technology.

The top six locations are:[6]

- United States,
- Dominican Republic,
- Colombia,
- Russian Federation,
- Brazil,
- Mexico.

This trend has led to a situation in which, even after huge investments by the EU banking industry to install hardware and software to accept EMV cards, the problem has become even bigger, as it is extremely difficult to prevent and investigate crimes committed outside of EU borders.

The ultimate solution to this problem would be to implement the EMV standard on a global level, including making United States' merchants compliant. Specific discussions on that are currently ongoing, however it is difficult to predict if, and when, the final stage of compliance might be reached.

As a short term solution, in October 2010 Europol and the European Central Bank recommended that all SEPA (European-issued) cards should be EMV (chip-embedded) only. The first Member State to follow this recommendation is Belgium (BE), where debit cards have chips embedded and the magnetic strip is no longer active. This solution, called GeoBlocking, in practical terms limits the possibility to misuse debit cards in regions without Chip and PIN verification. The implementation of GeoBlocking has been extremely positive from a security point of view with significant falls in skimming incidents and skimming-related losses (a decrease to almost zero in Belgium).

It should be stressed that there are some constraints to such solutions. The baseline for branded cards is that the cards are accepted globally. From this perspective the chip-only cards are not in line with this policy. The use of GeoBlocked cards is also less convenient for card holders as the card must be activated every time before travelling to non-EMV compliant countries. According to a research poll carried out by EAST[7], 60% of customers would be in favour of the GeoBlocking solution, including 28% of respondents who would be happy to contact their banks to activate the magnetic strip on their cards, and 12% who would like to hold a chip-only card.

This compromise is the price that card issuers and card holders pay as a result of the criminal activities of organised networks. It can be concluded that organised criminal groups (OCGs) have already managed to affect the EU payment card market to the extent that the use of cards is not cheap for card issuers and is less convenient for cardholders.

4.2. Investigations into card-present (CP) fraud

In 2011, industry reported an increasing number of incidents against ATMs in the European Union – 20 244 compared to 12 383 in 2010[8] . The statistics include all types of attacks against ATMs, including skimming, using stolen cards or physical traps to obtain cash. According to reports provided by EU law enforcement authorities (LEAs), organised crime groups (OCGs) adjust their profiles and criminal techniques relatively quickly and smoothly. Not only can they produce skimming devices to bypass the latest anti-skimming technology but they also explore new possibilities, including cash traps, prepaid cards or malware, as a source of cash and card data.

[6] Source: EAST report – European Fraud Update 2012
[7] Source: EAST annual report 2012.
[8] EAST, April 2012 update.

This situation requires LEAs to have a good overview of the situation and to react quickly. Most criminal structures operate internationally so cross-border cooperation is a key to final success. Taking into account that suspects use specific countermeasures, corrupt police officers[9] and hire the best lawyers[10], investigative measures in such cases are very difficult. The criminals' use of sophisticated technical equipment forces investigative teams to cooperate closely with forensic experts – who can decode information and analyse seized electronic storage devices. Unfortunately, in most of these cases, investigative measures focus on the criminal activities taking place in the European Union (skimming, counterfeiting of payment cards). Law enforcement agencies and judicial authorities, being limited by legal provisions, time frames and financial restrictions, can rarely investigate fraudulent transactions performed overseas. In practical terms, investigative measures rarely lead to dismantling the whole criminal structure. Judicial authorities press charges mainly for the part of the criminal activities that are performed in the EU – which is usually considered as the preparatory stage and not always associated with any financial losses. Consequently, in the majority of such cases the sentences are relatively lenient and suspects can leave jail on bail. Even if some criminals from an OCG are arrested for a period of time they can be easily replaced by others so that the criminal group is still active.

As summarised above, global cooperation in such cases is very difficult and EU law enforcement agencies are rarely able to prepare and finalise a wide-ranging operation. However, if a global operation is launched and many members of the same OCG are targeted, it has a big impact on the security of payment card transactions in the EU.

In June 2011 a global operation, 'Night Clone'[11] was brought to a successful conclusion with almost 70 suspects arrested in the EU and overseas. The operation had a very big impact and, for several months, illegal activities of many other OCGs ceased.

[9] Member States (MS) reported arrests/investigations against police officers for informing criminals about PCF cases.
[10] EU MS reported that suspects arrested for skimming are often defended by expensive and influential lawyers.
[11] Night Clone – an international operation initiated by the Italian Police, supported by Bulgaria, US Secret Service and other EU Member States. The final stage was coordinated via the operational centre set up at Europol.

5. Card-not-present (CNP) fraud

Payment card data is the ideal illicit internet commodity as it is internationally transferable. Europol, in its report on Internet Facilitated Organised Crime (iOCTA), concluded that organised crime groups (OCGs) clearly benefit from globalisation, using foreign payment card data to purchase goods and services on-line. Credit card information and bank account credentials are the most advertised goods on the underground economy's servers. According to Europol's intelligence, in 2011 around 60% of payment card fraud losses, totalling 900 million euros, were caused by card-not-present (CNP) fraud.

Within the major card-not-present fraud investigations supported by Europol, the main sources of illegal data were data breaches, often facilitated by insiders and malicious software. In most of these cases the quantity of compromised card details is substantial, reaching hundreds of thousands or millions, enabling criminals to sell the bulk data on the internet.

So far most of the credit card numbers misused in the EU have come from data breaches in the US. However, since 2010, Europol have observed a growing number of financial data breaches against EU-based merchants and card processing centres. Most of the investigations into these breaches are based on information on illegal transactions carried out using compromised cards, as the reporting of such attacks by the affected companies is still a weak point.

A major problem in the EU is the lack of proper regulations for reporting data breaches to police authorities. Law enforcement agencies, even if aware of a breach, have difficulties finding information on, and links to, the point of compromise, stolen data and illegal transactions. The lack of legal provisions on reporting data breaches is not the only problem. One of the key factors making industry reluctant to report incidents to law enforcement authorities (LEAs) is the lack of trust in investigative possibilities as well as the need to maintain the reputations of the respective private entities. On the other hand, the lack of reporting leads to a small number of international investigations and a low level of prioritisation of such cases within LEAs. The problem ends up with the situation where, despite a dynamic increase in CNP fraud, it is not reflected in the statistics of cases reported and investigated by EU police forces. Consequently, since the problem is not reflected in police statistics, this phenomenon is not prioritised and it is difficult to initiate international cooperation (for example Joint Investigation Teams) in such cases.

From the security perspective, as with the security of face-to-face transactions, there is a lack of a common global standards on the protection of card-not-present transactions. Major investments by EU industry have been made in the 3D secure protocol (MasterCard secure code; verified by VISA). However, despite this strong 3D secure verification, it is not a worldwide solution and, even on the EU level, not all on-line transactions are protected with it.

Investigations into CNP fraud and its initial stage – data breach - is typically very demanding. As identified by Verizon[12], such cases are usually quite large and complex, often involving numerous parties,

inter-related incidents, multiple countries, and many affected assets. In addition to that, as stated earlier, the majority of such cases are not reported to LEAs, as industry mainly focuses on preventive measures rather than relying on the outcome of investigations. The results of internal inquiries are used to improve security measures and rarely focus on the identification of individuals responsible for the breaches.

As far as investigations into illegal on-line card transactions affecting the EU are concerned, they are mainly concerned with:

- illegal ordering of high value goods on the internet;
- combating networks of mules set up to receive and transfer goods ordered on the internet;
- illegal transactions – purchases of services from travel companies/airlines;
- physical transactions with counterfeit credit cards – with data sourced from the internet;
- investigations into OCGs from the Baltic states and South East of Europe;
- the proper coordination of information – where possible, data breaches should be linked to illegal transactions;
- assets seizure – the network of mules shall be determined in order to localise the entry/exit points of goods.

[12] Verizon 2010 Data breach investigation report.

EU Member States (MS) reported many constraints and challenges faced during such investigations. The lack of legal provisions for reporting on-line incidents and data breaches, which are usually of an international nature, creates problems in individual cases under the responsibility of the respective MS, including the possibility to connect illegal transactions reported by other countries and decisions on the place of final prosecution. The global dimension and protection of financial and personal data is a major problem as far as the efficiency and time-frames of investigations are concerned. From a practical perspective, the involvement of Russian-speaking, well organised and hermetic structures cause huge problems with regards to infiltrating individuals and collecting evidence on their criminal activities. Since the majority of criminal activities are on-line (internet–based), the best solution is to task specialised cybercrime teams with such cases.

As there is still little experience on such card-not-present fraud cases – where data breaches and illegal transactions make EU companies and consumers the key targets – the role of Europol is crucial, to analyse information and spread strategic and operational information, ultimately ensuring the efficiency of investigative measures.

6. Final remarks

The financial crisis has had a big impact on the approach of private financial services companies and law enforcement authorities (LEAs). Currently, all decisions are thoroughly scrutinised and assessed from an economic and 'priority' perspective.

Private industry, as the money-driven entities, focus on products and services which bring profit in the first instance. Such companies can accept a certain level of fraud without making any effort to identify the individuals responsible for that fraud. From the law enforcement perspective it is increasingly suggested that, since losses caused by payment card fraud can be easily covered by private industry, there is no point in investing resources on investigations. The problem is even bigger as investigations must be performed on an international level, so the investment must be higher and comes with no guarantee of final success or seizure of assets.

All that leads to the dangerous situation in which the illegal income for members of organised crime groups, reaching 1.5 billion euros a year, is not identified and recovered. It seems that the EU response to the payment card fraud problem is not harmonised or fully supported by all actors – card schemes, card issuers, processing centres, law enforcement agencies and judicial authorities.

The EU still has to rely on outdated technology which does not adequately protect payment card transactions. One policy option available to strengthen security levels is to abandon the magnetic strip on payment cards for internal EU transactions.

As far as new technologies are concerned, including mobile or contactless payments, it is still not well analysed but there are certain doubts about their properly coordinated and standardised implementation to guarantee resistance to fraud.

The coordinated approach of industry and LEAs should lead, not only to the security of non-cash payments, but should also make sure that all incidents, including data breaches, are reported for further investigation. The position or reputation of the reporting entity should be protected and should not be undermined based on such a report.

Taking into account the global dimension of the problem, law enforcement and judicial authorities should take necessary steps to increase knowledge and awareness on the investigative skills and possibilities available. The role of Eurojust, as the agency for judicial cooperation, is extremely important to coordinate investigations and ensure the efficiency of prosecution and assets seizure in such cases.

Proper coordination of information – processing and reporting to the involved countries – is critical for efficient investigations. A centralised database is very important to link members of criminal networks, fraudulent incidents and investigations. Europol, having a specialised team with an existing operational database and a newly-created technical platform, can play an important role in such cases. The missing links that remain are the legal solutions on cooperation with non-EU States and the communication of data with private industry.