Fraud in cash and electronic payments: taxonomy, estimation and projections

A report for the International Security Ligue

Santiago Carbo-Valverde
Francisco Rodriguez-Fernandez

Executive summary

This report offers two main contributions. First of all, it provides a comprehensive taxonomy of payment fraud alternatives. Second, it offers an empirical estimation of the value of fraud with different cash and card payments, as well as some insights into the impact of new forms of electronic transactions, such as contactless payments and cryptocurrencies. The analysis suggests that payment fraud is a growing phenomenon, because technological efforts to curtail fraud practices are facing an even larger variety of fraud innovations that exploit vulnerabilities on two fronts: technological flaws (i.e. security gaps of devices/software) and social engineering (i.e. limited control of human-machine interactions).The concerns have been mostly considered in the aftermath of the crisis, as the more traditional fraud types (lost and stolen, counterfeit) were replaced by intangible new types of fraud. Overall, a significant shift from cash fraud to card-related fraud has also been observed.

The empirical analysis was conducted for the period 2014–2018 in 52 countries in Europe, North America, Central and South America, Asia-Pacific and Africa. In addition, the report provides some projections on fraud for 2025.

We highlight the importance of distinguishing fraud connected to tax evasion but derived from activities with a legal productive origin from fraud attached to illegal and non-productive activities. Importantly, the empirical evidence in this report indicates that cash related to illegal activities represents less than one fourth of the underground economy and this figure has recently been falling substantially. However, other forms of fraud, such as card-not-present (CNP), have increased by more than six times between 2014 and 2018 alone. The faster growth of card fraud compared to cash fraud has been compatible with a high demand for cash during a period of low interest rates in many jurisdictions. As demonstrated by the report, this persistent demand for cash has increased the structural (legal) component of the demand for currency. Since 2014, fraud with cash decreases and fraud with cards increases. According to our estimations, fraud with cash has been decreasing 1.7% annually while fraud with cards have been increasing 16.2% annually. If current trends persist, card fraud per transaction would double by 2025, while the illegal economy linked to cash would fall by 10.4%. As technology evolves, there is a diversification of payment channels and options. This has been particularly acute in the aftermath of the crisis, when social engineering has emerged as a substantial public policy problem. While technology improves security in certain segments, others risks emerge. This has been the case with the EMV chip in payment cards. As the EMV chip has been implemented in many countries, a transfer from ‘lost and stolen’ and ‘counterfeit’ fraud to CNP fraud has been observed.

As a general conclusion, our analysis suggests that fraud does not constitute an intrinsic characteristic of payment instruments, but represents a social problem that needs to be addressed with the appropriate public policies and private efforts. The empirical evidence revealed by the report indicates that, as other electronic payment instruments have been growing alongside cash, a significant share of fraud has moved from cash to electronic means of payment. While due to data availability and complex identification problems the quantitative analysis in the report does not include other fraud alternatives such as money laundering with cryptocurrencies, sales suppression devices or direct debit/credit transfer fraud, we survey some anecdotal evidence that suggests these are also quite significant fraud practices.

Quantitative highlights of the study

- The illegal economy linked to cash in 2018 was 0.93 times the value of 2014. However, total card fraud per transaction almost doubled (1.82).

- Fraud with cash has been decreasing 1.7% annually while fraud with cards have been increasing 16.2% annually.

- While the total shadow economy remained relatively stable during the period (ratio 2018/2014 = 0.99), the illegal economy linked to cash shrunk (0.93). This happened despite a general increase in the demand for cash (1.18) and on the ratio of transferable deposits over total deposits (1.20).

- Less than one fourth of the global underground economy is due to money laundering or illegal activities managed with cash.

- Globally, the illegal economy linked to cash has declined from 5.2% of gross domestic product (GDP) in 2014 to 4.8% of GDP in 2018. This component is particularly low in North America (2%) and Europe (3.3%) and larger in Central and South America (7.4%), Asia-Pacific (5.7%) and Africa (9.6%). In any event, it has declined in all areas during the period considered.

- The percentage of the illegal economy linked to cash has increased in countries that have traditionally maintained lower levels of cash usage. In Norway it reached 4% of GDP in 2018, and 3.4% of GDP in Sweden. In Finland (2%), it remained at similar levels to other more cash-incentive countries such as the United States (2%) and France (1.9%).

- Card-not-present fraud grew more than any other type of fraud. It was 6.44 times larger in 2018 than in 2014. The introduction of the EMV chip in many jurisdictions reduced card 'lost and stolen' fraud but increased more than proportionally CNP fraud. Card-not-present fraud constitutes more than half of total card fraud.

- ATM-related card counterfeit also increased (ratio 2018/2014 = 2.23), while POS counterfeit declined (0.61).

1. Introduction and motivation

Fraud, generally and simply defined as the crime of cheating in order to get money or goods illegally, is estimated to cost the global economy $4.1 trillion annually (Crowe, 2019). Payments, as the means for economic transactions, have been associated with fraud due to various security failures, malfunctions and malpractices. For some time, most analyses of fraud and means of payments have focused almost exclusively on cash. However, as technology has evolved, electronic payments have increasingly gained substantial attention.

This report offers an overview of the main types of payment fraud and the main public and policy concerns around them. It also provides estimations of the value of fraud committed based on different cash and card payments, as well as some insights into the impact of new forms of electronic transactions, such as contactless payments and cryptocurrencies. The empirical analysis was conducted over the period 2014–2018 in 52 countries in Europe, North America, Central and South America, Asia-Pacific and Africa. In addition, the report provides some projections for payment fraud in these locations by 2025.

As with other payment instruments, there are some myths and legends about fraud that do not correspond to the reality or the core of academic/expert analyses. These myths are the subject of transversal critical analysis throughout this report. Three important lessons are derived from this analysis:

i) Fraud does not constitute an intrinsic feature or aim of any payment instrument, but is a social problem that needs to be addressed with the appropriate public policies.

ii) As technology evolves, there is a diversification of payment channels and options and, subsequently, a growth of tech-related fraud channels.

iii) There is a need to distinguish fraud related to tax evasion but derived from activities with a legal productive origin from fraud attached to illegal and non-productive activities.

By way of preview, this report indicates that the number of ways to commit fraud is growing in line with the variety of electronic payment alternatives. Although innovation allows practitioners to prevent some types of fraud, there is also 'innovation' by fraudsters. They identify vulnerabilities in payment systems and how to exploit these. A particularly relevant case in recent years is the so-called card-not-present (CNP) fraud. As the Europay, Mastercard and Visa (EMV) chip has been implemented in many countries, a transfer from 'lost and stolen' or 'counterfeit' fraud to CNP fraud has been observed. In addition, although data availability does not permit a precise quantitative assessment of the impact on fraud using some relatively new forms of payments, there is anecdotal evidence suggesting that there are cases that indicate a significant real economic impact: sales suppression devices and cryptocurrencies.

From a quantitative viewpoint, this report estimates that money laundering and other illegal activities attached to cash have declined by 7.25% globally between 2014 and 2018. However, card fraud per transaction was 1.8 times higher in 2018 than in 2014 and some specific card-fraud types, such as CNP, are 6.4 times higher. While the weight of cash in the shadow economy is still quantitatively higher compared to other forms of payments – partly because its weight as payment instrument is also higher in the legal economy – it has declined over the period analysed in this report. Our projections suggest this trend will continue, as we offer a forecast up to 2025.

The report is divided into six sections. Following the introduction, Chapter 2 explains the main fraud types. Chapter 3 summarizes them, describes the related social problem and builds a taxonomy map of payment fraud. Chapter 4 explains the methodology to estimate payment fraud in 52 countries and discusses the results. Chapter 6 offers some projections for 2025. The report ends with the main conclusions in Chapter 7.

2. Fraud types: a growing variety of alternatives

2.1. Cash-related fraud

The definition of cash-related fraud appears simple. However, there are some specificities and distinctions that are not always appropriately considered. Cash fraud is mostly related to counterfeit, tax evasion and money laundering, but while counterfeit and money laundering are clearly labelled as illegal activities with no productive origin, not all counterfeit and money laundering is cash related. Money laundering is defined as '*the process by which criminals conceal or disguise the proceeds of their crimes or convert those proceeds into goods and services. It allows criminals to infuse their illegal money into the stream of commerce, thus corrupting financial institutions and the money supply, thereby giving criminals unwarranted economic power*' (FBI, 2011). It is true that cash is different from other payment instruments in that it guarantees anonymity, but many money laundering acts are not cash-based, as the setting up of anonymous shell companies in tax havens can then be used to set up anonymous bank accounts.

Tax evasion also requires further explanation. Avoiding taxes is a general purpose or consequence of many illegal activities. As noted by Ardizzi et al. (2014b), '*since cash in-flows are at least partially attributable to criminal proceeds that need to be laundered, what one must do to estimate the size of money laundering is to distinguish illegal proceeds from criminal activities and from other determinants of in-flows, including legal and illegal profits from tax evasion. In other words, one needs to run a decomposition exercise and identify the share of cash in-flows attributable to each of their determinants.*' Hence, it seems reasonable to distinguish illegal tax evasion activities with a non-legal origin (money laundering) from other activities that have a legal basis but are ultimately not reported for tax purposes.

The composition of tax evasion is critical to determine the extent to which cash is used for illegal activities with no real (or positive) economic impact from other activities with a real economic impact but tax evasion (see Figure 1).

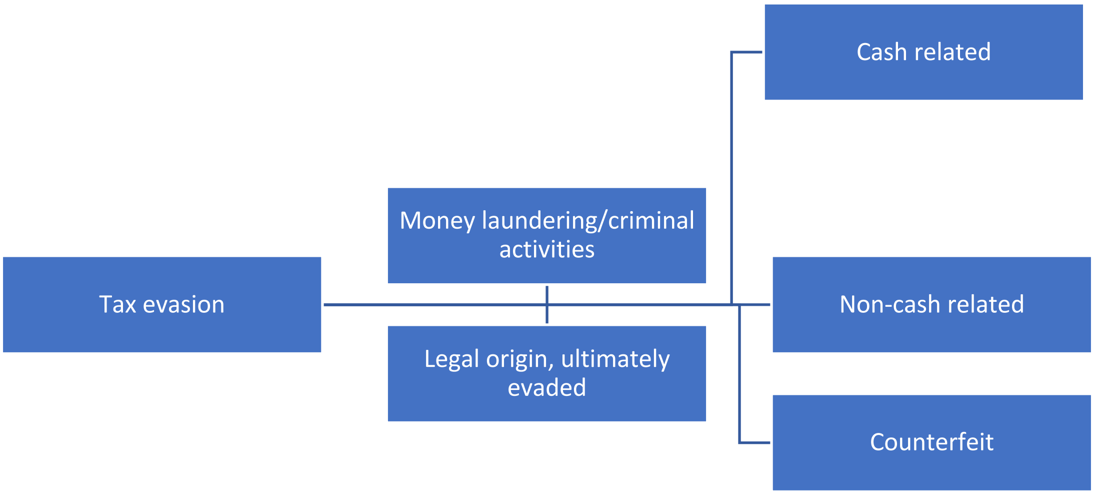

Cash related
Money laundering/criminal activities
Tax evasion
Non-cash related
Legal origin, ultimately evaded
Counterfeit

Figure 1. Tax evasion and cash: two different concepts

Source: Author's own elaboration

2.2. Electronic payment fraud

2.2.1. Grounds and social engineering

Technology offers a variety of electronic payment alternatives that translate into a wide range of fraud alternatives, with three main origins (see the schematic in Figure 2): internet-related fraud; e-commerce-related fraud and electronic payment fraud. These three methods are usually connected. Internet fraud is the use of internet services or software with internet access to defraud victims or otherwise take advantage of them.

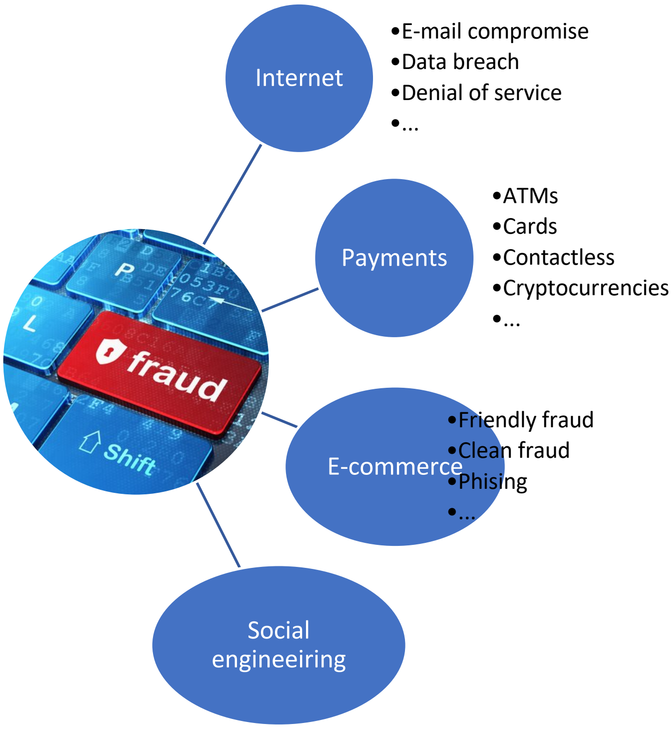


Figure 2. Intersection of e-fraud origins, methods and transactions

Source: Author’s own elaboration

According to the FBI's web page,[1] the internet incorporates several high-profile methods for this purpose:

- Business email compromise (BEC): A sophisticated scam targeting businesses working with foreign suppliers and companies that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to effect unauthorized transfers of funds.
- Data breach: A leak or spill of data which is released from a secure location to an untrusted environment. Data breaches can occur at the personal and corporate levels and involve sensitive, protected, or confidential information that is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.
- Denial of service: An interruption of an authorized user's access to any system or network, typically one caused with malicious intent.
- Email account compromise (EAC): Similar to BEC, this scam targets the general public and professionals associated with, but not limited to, financial and lending institutions, real estate companies, and law firms. Perpetrators of EAC use compromised emails to request payments to fraudulent locations.
- Malware/scareware: Malicious software that is intended to damage or disable computers and computer systems. Sometimes scare tactics are used by perpetrators to solicit funds from victims.
- Phishing/spoofing: Both terms refer to forged or faked electronic documents. 'Spoofing' generally refers to the dissemination of emails which are forged to appear as though they were sent by someone other than the actual source.

[1] See the specific FBI web page on Internet fraud: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud

‘Phishing’, also referred to as ‘vishing’, ‘smishing’, or ‘pharming’, is often used in conjunction with a spoofed email. It refers to the act of sending an email falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information, after directing the user to visit a specified website. However, the website is not genuine and was set up only as an attempt to steal the user's information.

- Ransomware: A form of malware targeting both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through spear phishing emails to end users, resulting in the rapid encryption of sensitive files on a corporate network. When the victim organization determines that they are no longer able to access their data, the cyber perpetrator demands the payment of a ransom, typically in virtual currency such as Bitcoin, at which time the perpetrator will purportedly provide an avenue to the victim to regain access to their data.

With the increasing popularity of e-commerce, a large proportion of payment fraud has moved to commercial transactions over the internet. However, electronic payment fraud and e-commerce fraud are not synonymous. There are several electronic payment fraud methods that occur in person or are directly connected to physical devices such as automated teller machines (ATMs), point-of-sale (POS) machines, or payment cards themselves. E-commerce fraud is an illegal or false transaction made via the web.

The important difference between physical and online payment fraud is that the card does not need to be present; CNP fraud is fast accounting for the lion's share of card payment fraud. According to a Nilson report on card payments (Nilson, 2019), card fraud has increased every year since 1993 and, in particular, since 2010. Card fraud losses increased by 17.7% in 2018 alone. The proliferation of card fraud cases and types is partially explained by the fact that it is hard to detect online fraud and catch the responsible fraudster.[2] The sources of potential fraud are multiple and that also introduces complexity. Some important distinctions attached to online fraud include the following:

- Friendly fraud versus clean fraud: In the case of friendly fraud, a buyer falsely complains and claims a refund for a purchase, keeps the purchased item and gets a refund, arguing the product never arrived, arrived in a bad condition or was bought with a stolen card. Clean fraud mainly consists of using a stolen card to do an online transaction. Various forms of this 'clean' alternative are described later in this report.
- Cross-border nature: Many of the online fraud practices are of a cross-border nature, which makes detection more difficult.
- Delivery chains are compromised: In some instances, third parties in a delivery chain are commissioned to re-ship products purchased with stolen card information. They never get paid and, in many cases, end up being liable for the fraud.
- Triangulation: In some instances, the fraudster creates a fake online storefront to sell goods at intentionally loss-making or very cheap prices. The only purpose is to access credit card data that is ultimately used for clean fraud purposes.

These online payment scams generate an immediate economic effect, the chargebacks. They represent a cost that also derives from other operational costs

[2] See Clearhouse blog entry: https://www.clearhaus.com/blog/fraud-in-ecommerce/

such as transaction fees, legal fees, or currency conversions. In a non-trivial number of cases, the merchant also loses the goods and assumes the cost of that loss.

Importantly, the European Payments Council (EPC) has defined the intersection of internet, e-commerce and payments as a form of social engineering (EPC, 2019). They define social engineering as ‘the art of manipulating people so they give up confidential information or their card / security device.’ This involves all kinds of illegal actions, from enticing individuals to give their credentials or other sensitive information to accessing personal devices to secretly installing malicious software. These practices make electronic payment fraud forms of behavioural problems that have become an important subject of study for psychologists and behavioural economists as, among other actions, criminals try to exploit an individual’s natural inclination to trust.

According to the EPC, customer authentication methods are a category on their own. Current electronic channels for economic transactions include passcodes, chip-card-based methods (e.g., EMV) or double identification methods (e.g. through email or short message service (SMS)). The EPC describes a wide range of social engineering practices that are used internationally. The following represent a summary of those most related to electronic payments:

- Email from a friend: This consists of accessing someone’s email password to obtain that person’s contact list. The criminals use the list or leave messages on the friends’ social pages, including a link the victims should trust and click, causing an infection of their devices with malware so that the criminal can take over their machines and collect information. Sometimes they ask for donations to a charitable fundraiser or some other cause.

- Recovery agent fraud: This happens when former fraud victims are told the money they have previously lost can be recovered. The fraudster claims to be a legitimate organization, alleging they can apprehend the original fraudster and recover the losses for a fee. When the fraud victims pay these fees, the fraudsters will keep coming back with another fee that has to be paid before the money can be returned.
- Phishing attempts. An email, instant message, comment, or text message that appears to come from a legitimate source explains there is a problem that requires the receiver to 'verify' information by clicking on a link. The fraudsters then ask for details such as an account number, password or card PIN. With this method, it is becoming very typical to create fake access points in high-traffic public locations such as airports or malls. Once the connection is made, the fraudster tracks the network traffic and possibly identifies valuable information to make payments.
- Fake applications (apps): These consist of the installation (on a computer or smartphone) of a fake user interface that substitutes a genuine app (bank or any other transactional app) when it is opened by the customer.

According to the FBI Internet Crime Report (FBI, 2019), BEC/EAC complaints proliferate and the US alone has officially registered losses of over $1.7 billion. Non-reported losses may imply a much larger figure in reality. According to the report:

> *BEC/EAC is constantly evolving as scammers become more sophisticated. In 2013, BEC/EAC scams routinely began with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers, and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. Over the years, the scam evolved to include compromise of personal emails, compromise of vendor emails, spoofed lawyer email accounts, requests for W-2 information, the targeting of the real estate sector, and fraudulent requests for large amounts of gift cards. In 2019, the IC3 observed an increase in the number of BEC/EAC complaints related to the diversion of payroll funds. In this type of scheme, a company's human resources or payroll department receives an email appearing to be from an employee requesting to update their direct deposit information for the current pay period. The new direct deposit information generally routes to a pre-paid card account.*

Although it is difficult to determine where the main threats will come from in the next few years, the combination of human and machine interactions may provide further risks of social engineering. The Proofpoint Human Factor Report 2019 (Proofpoint, 2019) provides a number of interesting details:

- More than 99% of internet threats observed during 2019 required human interaction to execute (e.g. opening a file, following a link).
- The top malware families during 2018 and 2019 consistently included banking trojans, information stealers, remote access trojans (RATs), and other non-destructive strains designed to remain resident on infected devices and continuously steal data that can potentially provide future utility to threat actors.

- Education, finance, and advertising/marketing topped the industries with the highest average number of attacks.

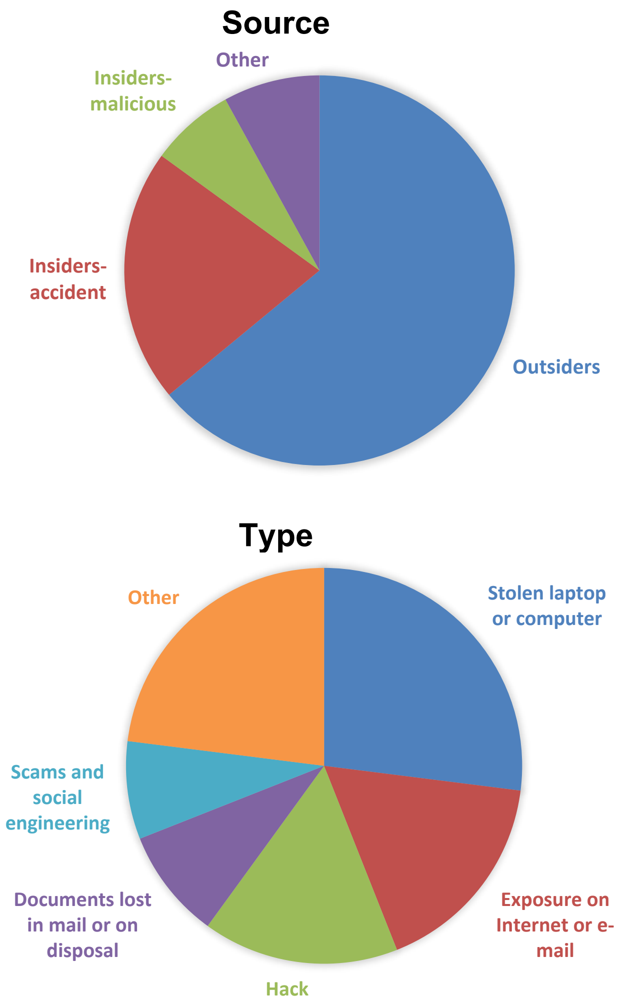


Figure 3. Data breaches in the United States: Source and type

Source: Sullivan (2010) and own elaboration

It is important to bear in mind that, until recently, insiders of an organization were mostly responsible for data breaches, but with the arrival of the internet, outsiders gained access to organizations' information. This change has been more evident in the post-crisis years. Sullivan (2010) has demonstrated that the majority of publicly disclosed data breaches are committed by outsiders, although insiders account for a significant share. Most incidents are the result of stolen laptops or desktop computers, followed by exposure of information on the internet or email and by hacking. Figure 3 illustrates the post-crisis scenario on the structure of data breaches in the US.

2.2.2. Automated teller machine fraud

The European Association for Secure Transactions' (EAST) guidelines offer a comprehensive list and definitions of ATM fraud methods (EAST, 2019):

- Card trapping: The unauthorized physical manipulation of an ATM, preventing the payment card being returned to the card owner. The criminal mounts a device over or within the ATM card entry slot prior to the customer using the machine and collects the card directly afterwards; the PIN can be obtained via shoulder surfing, camera or PIN-pad overlay.
- ATM-specific attacks (ATM malware/software related): The criminal runs unauthorized software, or authorized software in an unauthorized manner, at the ATM computer to perform an attack known as 'black box', that is, the fraudster connects an unauthorized device to an ATM that sends dispense commands directly to the ATM cash dispenser, effectively telling the machine to 'cash out'.
- Transaction reversal fraud: This refers to the unauthorized physical manipulation of an ATM cash withdrawal, which makes it appear that cash has not been dispensed, thereby causing a reversal message to be generated. The criminal requires an active payment card, approved for ATM usage and with sufficient available funds; they carry out a financial transaction and then physically manipulate the cash presenting sequence, either with or without the use of an unauthorized device. The criminal has gained access to, and removed, the cash, yet the ATM perceives that no cash was dispensed and passes a

reversal message for the issuer to complete. In these cases, the fraud losses are absorbed by the ATM owner.

- ATM skimming: Skimming refers to the installation of an unauthorized device to capture data from the magnetic strip of a payment card. The criminal manipulates the ATM or point-of-sale (POS) terminal, or attaches a skimming device to the card reader of the ATM or POS terminal; usually a PIN compromise device such as a micro-camera or PIN-pad overlay is installed at the same time.
- ATM shimming: Shimming refers to the interception ('passive') and/or manipulation ('active') of information flowing between an EMV card and the chip interface of a card reader. The objective is to obtain the original payment card and PIN details. Attempts at shimming devices on ATMs and POS terminals have been seen across the globe. The criminal targets issuers and/or acquirers who have not implemented the EMV protocol correctly.

Table 1. ATM device-related fraud types according to the European Association for Secure Transactions

Device	Description
M1. Overlay Skimming Device	The read head on this type of overlay device is external to the fascia and the motorized card reader throat (entrance) or covers the whole of the motorized card reader entrance.
M2. Throat Inlay Skimming Device	The read head on this type of device is placed inside the throat of the ATM or inside the legitimate bezel and in every case in front of the card reader shutter.
M3. Card Reader Internal Skimming Device	The read head on this type of device is placed at various locations inside the motorized card reader behind the shutter. This type of device is sometimes also referred to as a 'deep insert' skimming device.
D1. Overlay Skimming Device	The read head on this type of overlay device is external to the fascia and the dip card reader throat (entrance) or covers the whole of the dip card reader entrance.
D2. Throat Inlay Skimming Device	The read head on this type of device is placed inside the DIP card reader throat in front of the card reader read head.
D3. Card Reader Internal Skimming Device	The read head on this type of device is placed inside the DIP card reader throat behind the card reader read head.
E1. Pre-read Head Eavesdropping Device	This type of device is connected to the pre-read head of a motorized card reader.
E2. Read Head Eavesdropping Device	This type of device is connected to the read head of the card reader.
E3. PCB Eavesdropping Device	This type of device is attached to the PCB of the card reader.
E4. Communication Eavesdropping Device:	This type of device is connected to the communication interface (e.g. USB interface) of the card reader.
S1. Card Reader Internal Shimming Device:	This type of device is placed inside the card reader.

Source: EAST (2019)

The types of ATM fraud explained above provide a general classification of multiple technical possibilities. The EAST offers a more detailed typology, depending on the type of device used to enhance the fraud (Table 1).

Copying magnetic-strip track data at ATMs (also at POS terminals) by skimming is an important type of fraud in countries where ATMs are not protected by anti-skimming measures. While a cloned magnetic-strip payment card is difficult to use in countries where they are secured by EMV chip technology, this still represents a significant method. Moreover, shimming has emerged as a powerful alternative to counterfeit data from the (EMV) chip on a payment card. For instance, the European Payments Council reports that '*fraud can occur when card issuers have implemented the EMV specifications incompletely. Incidents in*

Europe have been seen but success is rare on the part of the fraudster due to the comprehensive implementation of EMV standards across Europe. However, in the U.S. and Mexico, due to the lack of implementation of EMV standards by issuers, fraud losses continue to occur related to shimming' (EPC, 2019).

2.2.3. Card fraud: counterfeit and lost and stolen

Counterfeit and lost and stolen are, perhaps, the basic traditional methods of card fraud. The few official statistics on this issue consider these the benchmark to determine the relative weight of other types of fraudulent acts with payments. These methods are particularly relevant in countries where transition to EMV chip cards has not been completed.

- Counterfeit card fraud: This is generally conducted following a skimming exercise. Specifically, a fake magnetic swipe card holds all the card details. This fake strip is then used to create a fraudulent card that is virtually a fully functional copy of the original card. Fraudsters can simply swipe it in a POS machine to pay for certain goods. A similar alternative is the so-called 'fake plastic', where the magnetic strip or chip on the card does not work but fraudsters attempt to convince a merchant that there is something wrong with the card and to process the transaction manually.
- Lost and stolen card fraud: This happens when cardholders lost possession of the card, either through theft or losing a card. As with counterfeit cards, the use of a stolen card may be limited if a PIN is required, but a frequent alternative is to make online purchases.

2.2.4. Card fraud: card-not-present fraud

- Card-not-present (CPN) fraud: This is perhaps the most important type of fraud with cards in recent years and refers to card transactions done by people who are not really in possession of the card. This is possible when someone knows the expiry date and account number of the card and can be done over the phone, or via mail or internet. Increasingly, merchants require the card verification code, making CNP fraud slightly more difficult. However, it is also true that fraudsters frequently access the verification code. Importantly, there are only 999 possible combinations for verification codes. For this reason, fraudsters may attempt to order items of very low amounts until they figure out the correct number.

The EPC (2019) notes:

> … *payment card details are obtained by fraudsters in various ways by malware or data hacks. When independent, small merchants set up their own online stores, a lack of knowledge around fraud risks can mean preventative measures are overlooked, which can leave those merchants open to greater risk of data hacking resulting in fraud. Hacking of large merchants continues to occur even though stores use protective measures. Criminals regularly find weaknesses and vulnerabilities.*

Among the most common cases of data breaches, the EPC mentions the ‘tour operators online’, a massive scam linked to fake travel agents. They also report that card data are frequently stolen in transit and that manually entered transactions (via CNP or without a PIN) are more frequently connected to hotel environments and clothing.

In recent years, in particular CNP fraud related to ‘account testing attacks’ has increased. The EPC describes this as –

> *an attack where a malicious actor may try to test if a card primary account number (PAN) exists, test CVVs or expiry dates related to a certain PAN, or try to inject any transaction with doctored fields to try to fool the authorization system in accepting the transaction as valid. Account testing attacks can be of various types […] These attacks can be performed through the transaction authorization systems or through the ACS enrolment verification systems. Account testing attacks can harvest millions of card credentials if no fraud detection system, with the capability to intercept transactions, is in place. Attacks have been detected where accounts are tested at great speeds (12 per second).*

Similarly, Sullivan (2010) has conducted a survey of these types of attacks in the United States and concluded that –

> *the payment cards that issuers provide are not sufficiently difficult to counterfeit. To accommodate merchants and consumers, card issuers continue to allow payments via mail order, the telephone, and now the Internet, with only the information from a payment card. Some merchants do not properly check payment cards for counterfeits or review signatures of cardholders. Some consumers write their personal identification numbers (PINs) on their payment cards or do not sufficiently protect their personal computers. Criminals take advantage of these and other vulnerabilities either to gather or to exploit information that lets them commit fraud […] Stolen data circulate among criminals in underground Internet markets. Evidence shows that stolen credit card information is most commonly available at a cost of $.85 to $30 per card number (Symantec). Bank account information is the second most common type*

> *of data available, at a cost of $15 to $850 per account number. Other information, such as full identities, online auction accounts, email accounts, and passwords are also for sale.*

Currently, there seems to be an overwhelming amount of CNP fraud in terms of total payment fraud. Shift Credit Card Processing[3] reports that in 2018, $24.26 billion was lost due to payment card fraud worldwide. They also indicate that the United States leads as the most credit-fraud-prone country, with 38.6% of reported card fraud losses, and that credit card fraud increased by 18.4% in 2018. Importantly, they report that CPM fraud '*is now 81 percent more likely than point-of-sale fraud and credit card fraud accounted for 35.4 percent of all identity theft fraud in 2018.*'

2.2.5. Card fraud: other[4]

- Application fraud: This happens when other people apply for credit or a new credit card in the name of another person. It can happen in multiple ways. In some instances, it is related to the stealing of, or unauthorized access to, the necessary personal supporting documents for card application.

- Mail non-receipt card fraud: This happens when a card is never received because it has been intercepted by fraudsters. The fraud is active when the interceptors are able to register the card and use it to make purchases or withdraw cash.

[3] Shift uses information from a variety of sources including experian.com; usatoday.com; www.cnn.com;
idtheftcenter.org; ftc.gov; nilsonreport.com; javelinstrategy.com; wallethub.com; or public.tableau.com (see https://shiftprocessing.com/credit-card-fraud-statistics/).

[4] See also ConsumerProtect (2018) for a classification of other types of card fraud https://www.consumerprotect.com/crime-fraud/11-types-of-credit-card-fraud-scams/

- Assumed identity: This happens when a criminal uses a temporary address and a false name to obtain a credit card.

- Doctored cards: This refers to a stored card whose metallic strip is erased. Fraudsters then manage to change the details on the card itself so that they match those of valid cards.

- Advanced persistent threat (APT): This refers mainly to cyberattacks or hacks targeted at specific stores or financial institutions, with the aim of compromising the network or payment system and gaining payment card data. Fraudsters can sometimes wait for months, ‘sleeping’ inside the system, before completing their attack.

2.2.6 Contactless payments fraud: an increasing problem

While apparently ‘lost and stolen card’ fraud should have diminished given the security-enhanced measures adopted by card companies (such as the EMV chip and CVV/CVV2), the contactless (NFC) facility on many cards and other electronic payment devices can also be used to obtain goods or cash under the card issuer’s contactless transaction ceiling or counter limit. Contactless payment cards are increasingly being accepted by merchants and adopted by consumers. These cards do not require authorization up to a certain number of transactions and up to a limited value. Although cardholders are progressively quicker to report their cards lost or stolen, the period before reporting may imply some losses that may be limited individually but are important at the aggregate level.

Juniper Research (2019) estimates that more than half (53%) of global transactions at point of sale will be contactless within five years, compared to just 15% this year. They consider that adoption will increase particularly significantly in the United States, with contactless going from less than 2% of transactions in 2019 to 34% by 2022.

Statista estimates that 48% of all point-of-sale payments in Europe in 2018 were already contactless.[5] According to Nets (2019), countries such as Denmark, where contactless represents a high proportion of card payments (56%), contactless fraud accounts for 65% of total card fraud.

The experience of the United Kingdom is also very illustrative. According to Action Fraud,[6] the UK's national fraud reporting service, £1.8 million was stolen from contactless users in 2018, compared to £711,000 in 2017. Fraudsters exploit the £30 limit. Equifax (2018) estimated that there were over 108.4 million contactless payment cards in circulation in the UK in 2018. The main *modus operandi* can be explained as follows:

> *Contactless cards contain both a chip and an antenna that is used to carry out the transaction. When you hold your card on or near a card reader, the reader sends out a signal which is picked up by the antenna. The chip inside contains information about your account and using this information, the reader can process its payment. Payments are currently limited to a maximum of £30 (previously £20) and are typically used for small retail purchases. There can sometimes be a problem with 'card clash' which is when two contactless cards, either payment cards or travel cards like Transport for London's Oyster Card, both interact with a card reader at the same time.*

[5] https://www.statista.com/statistics/946228/contactless-payments-market-share-at-pos-in-europe-by-country/

[6] https://www.actionfraud.police.uk/a-z-of-fraud/store-card-fraud

2.2.7. Credit transfer and direct debit fraud

The use of direct debit and credit transfers is particularly popular in some monetary areas such as the eurozone. Although Single Euro Payments Area (SEPA) accounts with high-safety payment infrastructures are conducted through banks, the European Payments Council (EPC) (2019) has detected a significant risk that current fraud practices may affect these payment alternatives. In particular, they suggest that –

> *during the last years, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continued to be the primary factor behind fraud losses related to these types of payments. In all of these methods, criminals target personal and financial details which are used to facilitate fraud.*
>
> *In an impersonation and deception scam, a criminal purports to be from a legitimate and trusted organization, such as a bank, the police, a utility company or a government department […] Fraudsters use a range of tactics to commit this crime such as sending fake invoices, offering fraudulent investment opportunities and online auction scams […] With regard to types of fraud, 'issuance of a payment order by a fraudster' remains the main fraud type for all SEPA payment instruments.*

2.2.8 The case of POS machine manipulation and tax evasion

One of the persistent myths of payment economics is that the shadow economy is almost entirely conducted with cash. Along with the critical comments on this view in section 2.2.1, it is important to consider that tax evasion is also spreading to electronic payment instruments. This refers to what the OECD

(2013) has called ‘electronic sales suppression’. It comprises all the techniques that facilitate tax evasion by electronic means and that ‘result in massive tax loss globally’. The Organisation for Economic Co-operation and Development (OECD) mentions four cases as examples of many others that may have occurred:

- Quebec tax losses for sales suppression are estimated at CAD417 million for 2007–2008.
- Sweden recovered €150 million in 2,000 audits over four years.
- In South Africa, €22 million was expatriated in a single case.
- In Norway, a single case involved €7 million being under-reported.

The problem is that there is no comprehensive record or statistics to identify the magnitude of the sales suppression problem. The sales suppression techniques are expected to contain the original data which tax auditors can inspect. These are elaborate frauds because of their ability to reconstitute records to match the skimming activity. Aimsworth (2019) points out that there is a demand market for technology that facilitates tax fraud and that ‘*by all accounts the providers in this market are working in a growth industry*’. He describes the two main technology accelerants of SME tax fraud: zappers and phantom-ware. Zappers and phantom-ware are programs that are added on (zappers) or factory installed (phantom-ware) to modern expense and cost recovery (ECR) or point-of-sale (POS) systems. The main purpose of zappers is to facilitate cash skimming at the point-of-sale. Phantom-ware may have legitimate (non-fraud) purposes, although these purposes are somewhat obscure (remote from normal business uses). As Aimsworth points out, ‘*phantom-ware programs are frequently hidden (in the sense of not being disclosed in user manuals), making their use* *and even their existence difficult to detect on audit. With training a fraudster can skim cash receipts with phantom-ware as effectively as with a zapper*.'

A related study by Aimsworth (2016) has focused on some cases detected in Canada and the United States. The evidence is based on police investigations into one of the main providers of these types of devices, InfoSpec/Profitek. It was a relatively 'popular' system used in the Canadian restaurant market that, at some point, migrated to the United States market. The investigation by Aimsworth describes the time gap between the beginning of the audit cycle involved in the InfoSpec/Profitek litigation in Canada – which started on October 4, 2000 – and the beginning of the first two similar investigations involving the same company and the same zapper in the United States, in 2014 and 2015. As Aimsworth points out, '*if the InfoSpec/Profitek system and its associated zapper crossed the U.S./Canadian border during the Canadian litigation, it would mean that this fraud was present and remained undetected in the United States for approximately fifteen years. This is a long time for fraud to remain hidden in the U.S. market.*'[7]

It is unclear what the economic impact of this fraud is, but the OECD assumes '*tax administrations are losing billions of dollars/euros through unreported sales and income hidden by the use of these techniques. Since the OECD's Task Force on Tax Crimes and Other Crimes (TFTC) began to work on and to spread awareness of this phenomenon a number of countries (including France, Ireland, Norway and the United Kingdom) have tested their retail sector and found significant problems. Among these countries, Ireland has moved quickly to put in place legislation to help tackle such abuse. Tackling this issue*

[7] The study describes how the FBI conducted an investigation in Chicago (public documents began to appear October 21, 2014), and the Washington State Attorney General also conducted another investigation (public documents began to appear July 13, 2015).

aggressively is seen by a number of countries as an important ingredient of a strategy to reduce their overall tax gap.'

It is not surprising that, following these events – and even if the total evasion figures remain unknown – some governments have reacted. The Canadian authorities passed a law in January 2014 regarding businesses that use, possess, or acquire electronic sales suppression (ESS) software, setting fines of $5,000 for the first infraction and $50,000 for any subsequent infraction. In addition, the law states that anyone who manufactures, develops, sells, possesses for sale, offers for sale, or otherwise makes available ESS software will face a $10,000 fine on the first infraction and a $100,000 fine on any subsequent infraction. Similarly, the Australian government passed a law in October 2018 banning any activities involving electronic sales suppression tools for people and businesses that have Australian tax obligations.

Some other countries are still trying to infer the magnitude of the problem. The UK government (HM Revenue and Customs) issued a call for evidence in December 2018, as there is no UK legislation that explicitly refers to ESS or the misuse of electronic POS systems.

Interestingly, Aimsworth (2019) refers to many other cases that may look anecdotal but may hide significant tax losses. As an example, he refers to 'TT PI Electronique', a cash register (hardware) that was used to skim cash sales. It is a French-made cash register that is a popular restaurant model in significant use in Italy, Belgium, Portugal, Spain, Germany, Denmark, Australia, the United States and North Africa. The software program operating the suspect cash register is called Restodata. In any case, it is difficult for tax administrations to identify the fraud, as it consists of a zapper system and, once a zapper is found, its trail only leads back to the single restaurant where it was found.

2.2.9 Fraud with cryptocurrencies

If there is a current case of electronic payment/channel that illustrates the threat of money laundering, it is cryptocurrencies. As with electronic sales suppression, fraud with cryptocurrencies is not considered in this report, for empirical purposes, due to the lack of information available that would be needed to build consistent estimates for the countries covered. However, there is some aggregate evidence that illustrates the importance of the method.

The identification of crypto-assets fraud is difficult, as there is no simple or reliable criterion to assign any of the possible illegal practices (e.g. money laundering) to a specific country. Ciphertrace (2020) tracks global fraud trends with cryptocurrencies and estimates that cryptocurrency user and investor losses due to fraud and misappropriation increased by 533% in 2019 compared to 2018. Losses stemming from fraud and the misappropriation of funds are estimated to have amounted to US$4.5 billion during 2019 alone. Notably, a quantitative analysis of all the transactions on the 20 top cryptocurrency exchanges globally revealed that 97% of direct Bitcoin payments from identifiable criminal sources were received by unregulated cryptocurrency exchanges.

One of the global references in anti-money laundering (AML) is the Treasury Department's Financial Crimes Enforcement Network (FinCEN) in the United States. E-money institutions, such as PayPal, Western Union and MoneyGram, must comply with the regulations adopted by FinCEN. However, cryptocurrencies are more difficult to regulate/supervise under the same framework. In principle, cryptocurrencies should comply with FinCEN's Bank Secrecy Act and other federal laws that ban unlicensed money transmitters. However, cryptocurrency operators argue that they are not a fiat currency but a bartering tool. Some cryptocurrencies have agreed to comply with FinCEN regulations while others have not.

As explained by DeAngelis and Associates, a firm specialized in security management and counterterrorism:

> *… the problem, of course, is that one can convert anything of value, including fiat currency, into Bitcoins simply by bartering or buying them. As a result, one could easily sell illegal services or products strictly for Bitcoins, or purchase large amounts of the digital currency with regular fiat currency, then transmit the digital currency offshore and either exchange it for more illegal products and services or convert it to another nation's fiat currency and deposit it into a bank. Through this process, one either avoids handling actual currency or simply converts it to fiat currency out of the country where the transaction will not be noted by the government and the associated criminal activity is less likely to be detected.*[8]

In June 2019, the Financial Action Task Force (FATF) of the United States Treasury released guidelines to combat money laundering and terrorism financing. The FATF encourages crypto exchanges and regulators around the world to comply with identification and transparency rules. The deadline to comply with these rules was set for June 2020.

The concerns of the United States Treasury are shared by the OECD. As demonstrated by Katarzyna (2019) –

[8] https://www.deangelisandassociates.com/post/what-is-the-threat-of-money-laundering-associated-with-bitcoin

> *… estimates of the amount of money laundered worldwide range from USD 500bn to a USD 1tn and such a procedure is not the problem of only a few nations: citing Basel AML Index, around 64% of countries have been classified as having a significant risk of money laundering with only 4% of countries able to improve their ranking comparing to their last year's results (2018). Since 2008 the illicit users have another tool, namely cryptocurrencies, which started to become a very promising mechanism for players wishing to engage in money laundering.*

The Economist (2018) has illustrated some of the ways in which cryptocurrency agents can launder money. In particular, there is the so-called 'micro laundering', in which small chunks of cryptocurrencies are exchanged for fiat and later deposited into regular accounts, causing them to look less suspicious (this has been identified as a method of European dealers to pay for Columbian cocaine). According to Europol statistics, around 3% to 4% of Europe's annual criminal takings is crypto-laundered ($4,2–5,6 bn). According to Chainalysis, over three quarters of 'illegal' cryptocurrency is moved through an online exchange service at some point. As they report, '*a majority of illicit funds actually flow through either exchanges, or peer-to-peer exchanges, with the rest flowing through other conversion services such as mixing services, [Bitcoin] ATMs and gambling sites.*'[9]

In Europe, crypto assets have also been identified as a growing source of money laundering. The Directorate-General for Internal Policies of the Union (European Parliament), in coordination with the FATF, has studied the

[9] https://blog.chainalysis.com

introduction of a new EU-wide anti-money laundering directive that covers cryptocurrencies. These efforts have been summarized by Houben and Snyers (2018). They indicate that the Fourth Anti-Money Laundering and Counter-Terrorism Financing Directive (AMLD4) did not capture the reality of transactions in cryptocurrencies. The problem is that '*none of the players in the cryptocurrency scheme, regardless of which cryptocurrency is concerned, is directly or indirectly included in the list of obliges entities, not even crypto exchanges. Therefore, the AMLD4 framework simply cannot be attached to the crypto scheme, exempting it fully from the AMLD4 scope*.'

Trying to fill the gaps of the AMLD4, the European Parliament approved the Fifth AML Directive (AMLD5) in July 2018. It requires crypto exchanges and custodial service providers to register with their local regulator and demonstrate compliance with thoroughgoing know-your-customer (KYC) and anti-money laundering procedures. In addition to the enhanced KYC and reporting obligations, the regime gives greater power and reach to financial intelligence units and law enforcement. Transposing the directive to the EU member states will be lengthy and complicated. The AML authorization schemes regarding crypto vary across Europe and this makes enforcement a complex issue. The AMLD5 intends to comply with the FATF recommendations. However, the AMLD5 covers only cash-to-crypto transactions and vice versa, while the FATF recommendations also include crypto-to-crypto exchanges.

3. A taxonomy of payment fraud: a significant social concern

3.1. The map

The discussion of the different sources of payment fraud invites to three types of classifications to build a comprehensive taxonomy[10]:

a) According to implications for tax collection:

a1) Payment fraud via tax evasion of activities with a legal productive origin.

a2) Payment fraud via tax evasion of criminal/illegal activities.

b) According to a comprehensive view of current practices (see Figure 4):

b1) Cash counterfeit

b2) Cash-related money laundering

b3) Counterfeit cards

b4) Card application fraud

b5) Card-not-present (CPN) fraud

b6) Lost and Stolen card fraud ((contactless included)

b7) Mail Non-Receipt card fraud

b8) Assumed Identity card fraud

b9) Doctored cards

b10) ATM Skimming

b11) ATM Shimming

b12) ATM/POS Advanced Persistent Threat (APT)

b13) ATM card Trapping

[10] A purely complete taxonomy is, by definition, very difficult given the dynamic "creative" nature of fraud activities, in particular of those related to technological innovations.

b14) ATM Malware/ Software-related

b15) ATM transaction reversal fraud

b16) Direct debit and credit transfer fraud

b17) POS electronic sale suppression

b18) Cryptocurrency fraud

c) According to a practical view of the current reality of statistical sources (mainly from central banks):

c1) cash-related fraud

c2) ATM lost and stolen

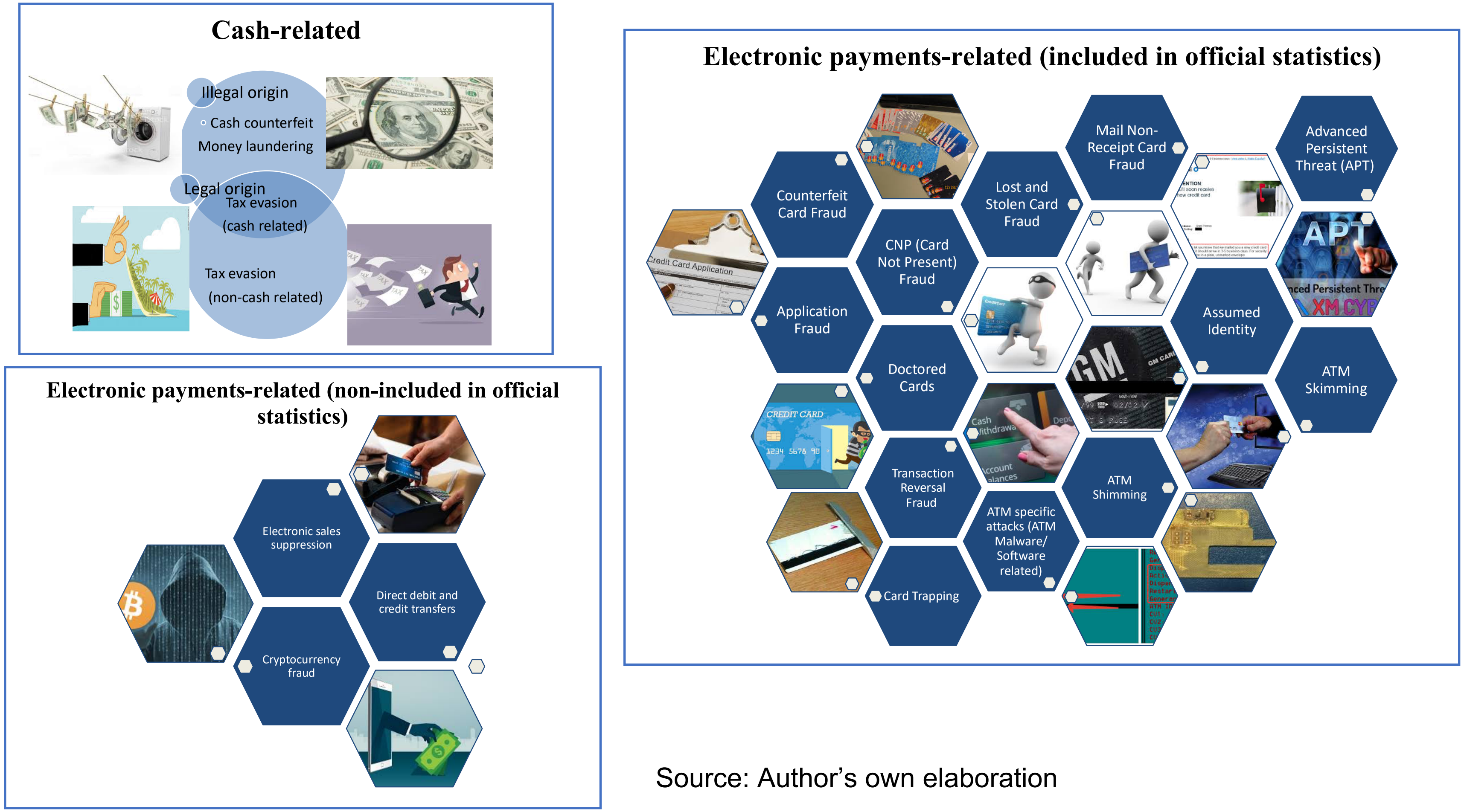
c3) ATM counterfeit

c4) POS lost and stolen

c5) POS counterfeit

c6) Card-not-present (CPN) fraud

Figure 4. A map of payment fraud based on a comprehensive view of current practices


Cash-related
Illegal origin
Cash counterfeit
Money laundering
Legal origin
Tax evasion
(cash related)
Tax evasion
(non-cash related)
Electronic payments-related (non-included in official statistics)
Electronic sales suppression
Direct debit and credit transfers
Cryptocurrency fraud
Electronic payments-related (included in official statistics)
Counterfeit Card Fraud
Application Fraud
CNP (Card Not Present) Fraud
Doctored Cards
Transaction Reversal Fraud
Card Trapping
Lost and Stolen Card Fraud
ATM specific attacks (ATM Malware/ Software related)
Mail Non-Receipt Card Fraud
ATM Shimming
Assumed Identity
Advanced Persistent Threat (APT)
ATM Skimming
Credit Card Application
CREDIT CARD
1234 5678 90
APT

Source: Author’s own elaboration

3.2. Digital payment fraud: a growing problem

Figure 4 illustrates the development, over the past 15 to 20 years, of a complex web of electronic payment fraud alternatives to cash. They are mostly linked to evolutionary cyber-sophistication and social engineering. This evidence and recent analyses suggest a few important characteristics of 21st century payment fraud:

i) It is a growing phenomenon because (public and private) technological efforts to curtail these practices are facing an even larger variety of fraud innovations that exploit vulnerabilities on two fronts: technological flaws (i.e. security gaps of devices/software) and social engineering (i.e. limited control of human-machine interactions). Juniper Research (2020) forecasts that banking and goods sales will constitute 76% of the e-commerce market by 2020. This trend exists in parallel to a growing number of fraud attempts. ACI Worldwide (2019) used e-commerce data from the United States to demonstrate that one out of every 85 transactions was a fraudulent attempt in 2017, while in 2016 the figure was one out of 97, and in 2015 one out of 109.

Aeorospike (2019) estimates that non-cash is likely to represent over one million transactions every minute by 2020. They report that although cards remain the dominant and fastest-growing payment instrument, the landscape is poised for rapid change and market disruption. They consider that –

> *… the growing adoption of mobile payments, particularly among millennials, combined with a rapid uptake in e-commerce 'card not present' (CNP) transactions, and the emergence of non-banking payment service providers (FinTech) are among the many factors causing turbulence and*

> *disintermediation in discrete parts of banking and the payments landscape*.

ii) The concerns have been mostly considered in the aftermath of the crisis as the more traditional fraud types (lost and stolen, counterfeit) have been replaced by intangible new types of fraud. Research by the Federal Reserve Bank of Kansas City (2010) indicates that these concerns were already observable from 2010 onwards. In particular, Sullivan (2010) notes:

> *Like all forms of payment, cards have security vulnerabilities. Traditional forms of card payment fraud are still an important threat, but fraud resulting from unauthorized access to payment data appears to be rising. Payment providers are exploring options to protect sensitive data, such as the recently implemented payment card industry data security standard. But the damage from card payments fraud is a rising concern, and we are only beginning to get a sense of the dimensions of the problem.*

What has changed in recent years for such a rapid transition to take place? According to Aerospike (2019), the digital world is aiming to displace cash, but this is also creating 'flash fraud' actions, which means a higher concentration of fraud transactions over shorter periods of time. The reasons would be the proliferation of digital payment alternatives, data-driven solutions permitting faster transactions and the proliferation of third-party access and not just banks dominating the system. That is probably why, according to LexisNexis (2019), merchants report that fraud losses are increasing, despite companies investing more in fraud prevention.

iii) The growing variety of alternatives suggests that fraud is not inherent to the payment instrument but a social problem that needs proper rules and enforcement. This has consequences not only for consumers, but also for merchants and banks. An important indicator of disruption in retail trade is the increasing number of chargebacks, which is a demand by a credit card company for a retailer to make good the loss on a fraudulent or disputed transaction. These have become an empirical regularity. LexisNexis (2015) reported that large e-commerce merchants in the United States, on average, lost 1.39% of revenue to fraud in 2015, despite spending around $115,000 annually on fraud mitigation. They also revealed that mobile commerce (m-commerce) and international e-merchants reported even higher fraud losses, at 1.68% and 1.58% respectively. With electronic fraud, merchants have to incur additional costs in areas such as shipping and insurance, investment and operational costs, manual review costs – costs of internal staff to review suspicious transactions – and chargebacks. As for banks, according the KPMG Global Banking Fraud Survey (KPMG, 2019), half of survey respondents globally had experienced increases in both external fraud total value and volume in 2018. The main contributing fraud types globally, from 2015 to 2018, included identity theft and account takeover, cyber attacks, card-not-present fraud and authorized push payments scams.

iv) Fraud prevention and fraud sophistication operate as communicating vessels. When a certain type of fraud prevention technique or instrument is applied, fraud flows to other ways of exploiting vulnerabilities of other payment instruments (e.g. as happened with the introduction of the EMV chip, which reduced card counterfeit but coincided with an increase in CNP fraud). Juniper Research

(2020) has, for example, analysed the United States market and demonstrated that fraud affects the entire electronic payments value chain, spreading rapidly across geographies and industries. In recent years, CNP fraud in particular has been on the rise and they suggest the main determinants have been the growth in e-commerce as a mainstream service, the increased number of serious data breaches – and technology introduction – and the fact that EMV introduction in the United States is switching fraudsters' attention to CNP purchases.

4. Estimating the size and evolution of payment fraud

4.1. Data and methodology

The aim of this section is to estimate the magnitude and evolution of payment fraud. One of the main assumptions of our study is that the concept of fraud should be consistent across types of payments (cash and electronic). Specifically, most fraudulent electronic payments in the scant official statistics are widely identified as those related to criminal activities such as theft and counterfeiting, with no productive origin. This excludes other types of fraud that may (or may not) have a legal origin but are finally tax evaded, such as sales suppression or cybercrime. In the case of cash, as illustrated in Figure 4, there are activities that have a legal origin but are tax evaded and other activities that are linked to criminal and non-productive activities with a fraudulent origin. We concentrate on the latter. Following this assumption, our analysis compares cash fraud with electronic payment fraud, relying on the classification of the taxonomy illustrated on page 33. The main reason for this choice is that our estimates can be compared with the figures offered by official bodies (mainly central banks) and, therefore, we can assess the reliability of our methods and to what extent they can be extrapolated to countries where these sources are scarcer or simply anecdotal. Therefore, the empirical analysis covers:

i) cash-related fraud;

ii) ATM lost and stolen;

iii) ATM counterfeit;

iv) POS lost and stolen;

v) POS counterfeit;

vi) card-not-present (CPN) fraud; and

vii) total card fraud (as the sum of ii, iii, iv, and v).

All the indicators are estimated for 2014–2018. With the definition of fraud employed, in line with official statistics and considering the information availability, three types of electronic fraud have been omitted from the empirical analysis: money laundering with cryptocurrencies, sales suppression with POS devices and fraud with direct debit/credit transfer.

Our sample covers 52 countries in four geographic areas (see Figure 5):

- EUROPE: Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia; Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom, Switzerland and Norway.
- NORTH AMERICA: The United States and Canada.
- CENTRAL AND SOUTH AMERICA: Brazil, Mexico, Colombia, Chile and Argentina.

- ASIA-PACIFIC: Australia, Japan, India, China, Malaysia, Thailand, Hong Kong, South Korea and Russia.

- AFRICA: South Africa, Nigeria, Egypt, Morocco, Zambia and Mozambique.

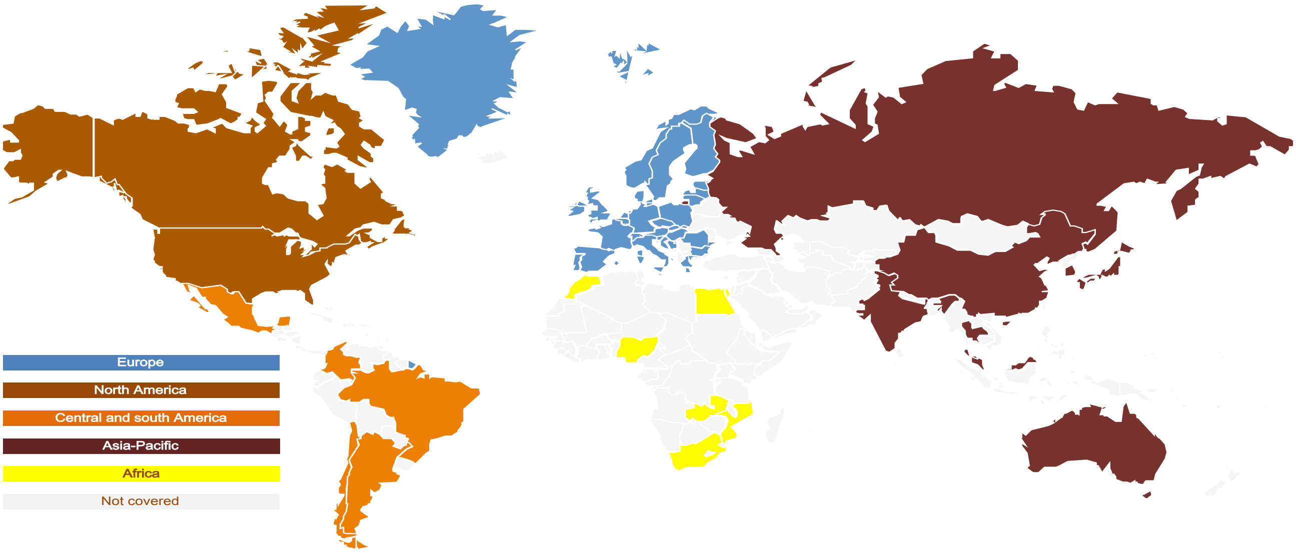


Figure 5. Areas covered by the study

Source: Author's own elaboration

The basic sources are the following:

- The Card Fraud Report published by the European Central Bank (editions from 2014 to 2018);
- The Networks, Processors, and Issuers Payments Surveys (NPIPS) of the Federal Reserve Board of the United States (editions from 2014 to 2018); and
- The Australian Payments Network Fraud Statistics.

In addition, the following non-regular reporting and anecdotal sources were also considered:

- The Canadian Mounted Police briefings on Credit Card Fraud;
- CardnotPresent.com reports on payment fraud in South Korea;
- Evidence on fraud in India from fundstiger.com, geminiadvisory.io, and digitalcheck.com;
- Data on Mexico and Brazil from central bank briefings, digitalcheck.com and Juniper (2020);
- Data on Zambia from Zambia Police briefings;
- Data on Nigeria from the Nigerian Electronic Fraud Forum (NeFF);
- Data on Thailand from Aite (2016), FICO-Thailand and central bank briefings;
- Data on China from Juniper (2020), Statista, digitalcheck.com, central bank briefings, and press reports;
- Data on Russia from Statista, FICO-Russia and Juniper (2020);
- Data on Japan from central bank briefings, Gemini Advisory and Juniper (2020);
- Data on Morocco from *The North Africa Post*, ravellin.com, and reportlinker.com;
- Data on South Africa for the South African Banking Risk Information Centre;
- Data on Malaysia from Bank Negara Malaysia; and
- Data on other countries from Juniper (2020), Nilson (2019) and Aite (2016).

Importantly, information was not available for all countries, years and fraud types and we had to estimate these from the available information, applying an econometric model to ‘fill the gaps’. In the case of cash, the figures are directly estimated from an econometric model. Both methods are explained in the next section.

4.2. Econometric models

4.3.1. Estimating cash fraud

Ardizzi et al. (2014a and 2014b) provide robust methodologies to estimate the share of the shadow economy that is related to criminal activities conducted with cash. It is what is called a ‘decomposition exercise’ to disentangle illegal proceeds from criminal activities from other determinants of money laundering with a legal origin. The methodology relies on mainstream research based on the demand for currency approach (CDA). Basic references in this area of particular interest for the purpose of our analysis are also Schneider (2002, 2007, 2010, 2011) and Fischer et al. (2004).

The CDA approach follows two stages to measure the shadow economy. First of all, it estimates an aggregate money demand equation, capturing (among other factors) the relationship between cash and the shadow economy. Second, the demand for currency linked to shadow transactions is then computed as the difference between the estimated demand for cash in the full model and the demand obtained by setting to zero all the determinants of the shadow economy. The final figure is the product of the estimated value of cash and the velocity of money proxied by the ratio of gross domestic product (GDP) to a relevant monetary aggregate.

Following Ardizzi et al. (2014b), we distinguished three components of the demand for cash:

- Structural component: natural demand for cash for legal purposes;
- Underground component: linked to tax evasion but with a legal productive origin; and
- Illegal component: underground from illicit non-productive criminal activities.

The demand for currency is estimated as the ratio of currency and demand in circulation to broad money (source: IMF). The structural component includes the per capita GDP, the unemployment rate, the ratio of transferable deposits to total bank deposits, the ratio of POS transactions to GDP and the interest rate on bank deposits (sources: IMF, World Bank). The underground component includes the tax burden measured as tax collection over GDP, the share of employment in agriculture over total employment and the share of employment in construction over total employment (sources: World Bank and OECD). The illegal component includes crime measured as the number of cases of drug trafficking, sexual exploitation, trafficking in weapons and explosives, and participation in an organized criminal group per inhabitant (sources: United Nations Office for Drugs and Crime, FBI and Interpol).

The summarized form of the equation would be as follows:

$$\textit{Demand for cash}_{it} = \alpha_0 + \alpha_1\ \textit{Structural}_{it} + \alpha_2\ \textit{Underground}_{it} + \alpha_3\ \textit{Illegal}_{it} + \varepsilon_{it} \quad (1)$$

The main equation was estimated for 52 countries (*i=1… 52*) over the period 2014–2018 (t=1… 5). The results are presented in Appendix A.

4.3.2. Estimating card payment fraud

As for payment card fraud, we estimated a model with the known data to help us compute estimates for the unknown data. In particular, card fraud per transaction, ATM fraud and card-not-present fraud were accommodated in a model where the explanatory variables include:

- Infrastructure variables: ATM transaction size, ATMs per inhabitant, POS transaction size, POS devices per inhabitant (sources: all from the World Bank and national central banks);
- Crime and underground economy variables: burglary and theft per inhabitant (source: United Nations Office for Drugs and Crime), employment in the retail commercial sector and in tourism over total employment (sources: World Bank and OECD); and
- A dummy variable capturing when the EMV chip was adopted (source: EMVco.com).

The equation is expressed as follows:

$$\begin{aligned}&\textit{Fraud variable}_{it} = \alpha_0 + \alpha_1\,\textit{Infrastructure}_{it} + \alpha_2\,\textit{Crime and underground}_{it}\\&+ \alpha_3\,\textit{EMV dummy}_{it} + \varepsilon_{it} \qquad (2)\end{aligned}$$

The main equation was estimated for 52 countries (*i=1… 52*) over the period 2014–2018 (t=1… 5). The results are also presented in Appendix A. For robustness check purposes, the estimated coefficients replicated, with a minimal error, the official figures of euro area countries that are publicly available and do not require any estimation effort.

4.3. Results

The following sections offer a breakdown of the results for the five geographic areas and the global average. Although some comments on specific countries are included, detailed results for the 52 countries are provided in Appendix B.

4.3.1. General trends for cash demand and the shadow economy

By way of preview, it is important to check the evolution of the demand for currency as the main reference to build the estimates of the shadow economy and cash fraud. Figure 6 reveals that globally demand for cash was 1.2 times higher in 2018 than in 2014. In Europe, the ratio was 1.4 and in North America it was 1.1. It remained flat in Asia-Pacific (ratio 2018/2014 = 1), while it fell in Africa (0.9) and Central and South America (0.8).

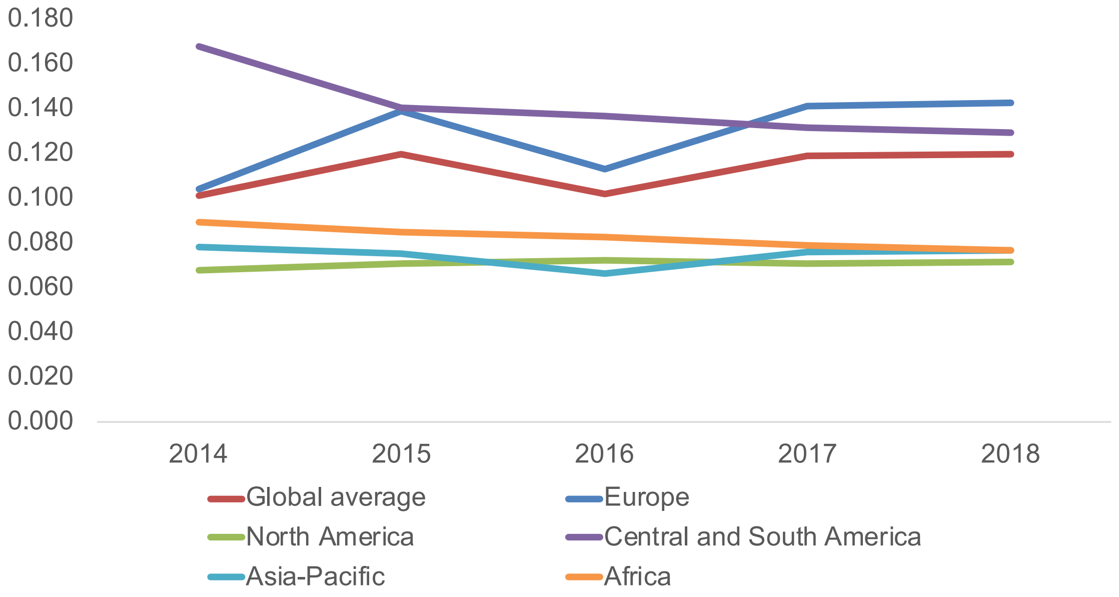


Figure 6. Demand for currency (currency in circulation to broad money)

Source: Author's own computation from sources described in section 4.3

The global increase in the demand for cash is related to the persistence of cash as a payment instrument and to changes in monetary policy that have generated very low interest rate environments in a number of areas and, in particular, in Europe and North America. Interestingly, this has also caused a shift in the demand for deposits from saving accounts to transferable deposits (Figure 7). This was 1.2 times larger globally in 2018 compared to 2014 and increased during this period in all areas, with the exception of Central and South America.

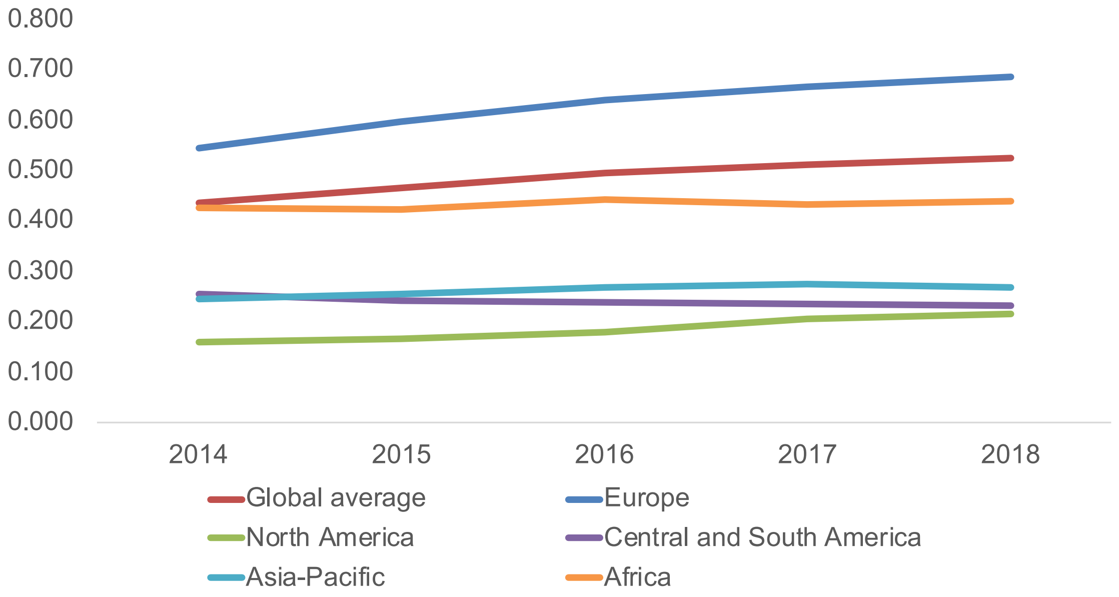


Figure 7. Transferable deposits to total deposits

Source: Author's own computation from sources described in section 4.3

This shift to demand deposits has to be taken into account as a particular feature of the period under study in this report and therefore was included as one of the explanatory factors in the structural component of the demand for cash equation. The results of the estimation of the shadow economy as a percentage of GDP are presented in Figure 8.

For the average of the 52 countries considered, the shadow economy represented 20.3% of GDP in 2018, falling slightly from 2014 (20.4%). Declines were observed in all areas, with the exception of Central and South America, where the estimated underground economy was 26% in 2014 and increased to 26.7% in 2018. The highest value was observed in Africa (34.7%), followed by Central and South America (26.7%), Asia-Pacific (20.8%), Europe (16.9%) and North America (8.5%).

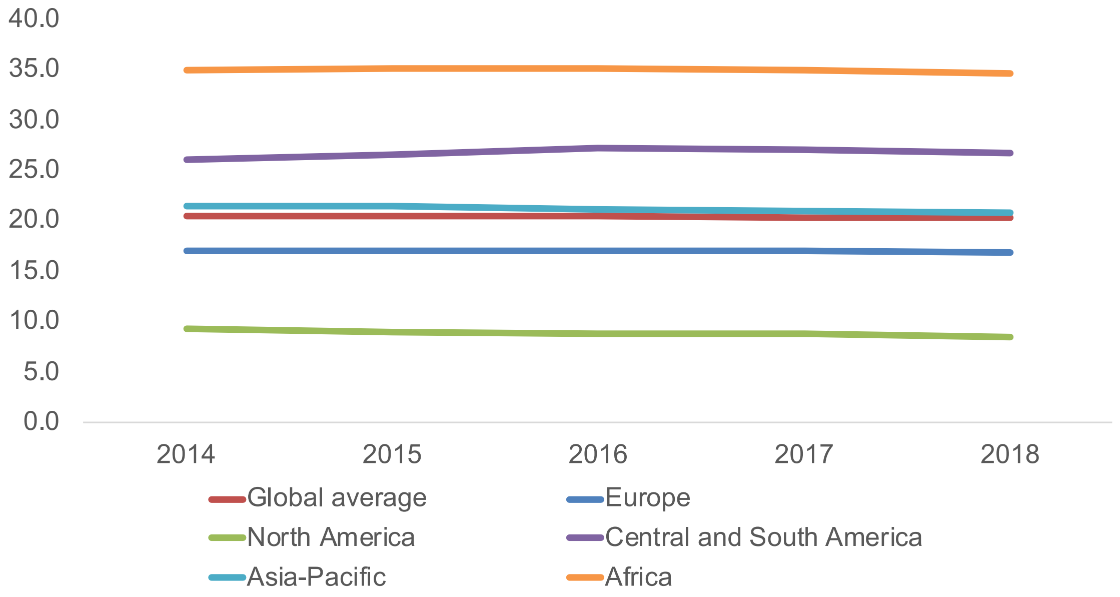


Figure 8. Estimation of the shadow economy as a percentage of GDP

Source: Author’s own computation from sources described in section 4.3

4.3.2. Cash fraud

As explained in section 4.3.1, the shadow economy can be broken down into a cash-related illegal component and an underground (tax evaded with a legal origin) component. Figure 9 illustrates the money laundering/illegal activities linked to cash over GDP. Various important general observations include the following:

- Less than one fourth of the global underground economy (23.6%) is due to money laundering or illegal activities managed with cash;
- The illegal economy linked to cash globally has declined from 5.2% of GDP in 2014 to 4.8% of GDP in 2018; and
- This component is particularly low in North America (2%) and Europe (3.3%) and larger in Central and South America (7.4%), Asia-Pacific (5.7%) and Africa (9.6). In any event, it has declined in all areas during the period considered.

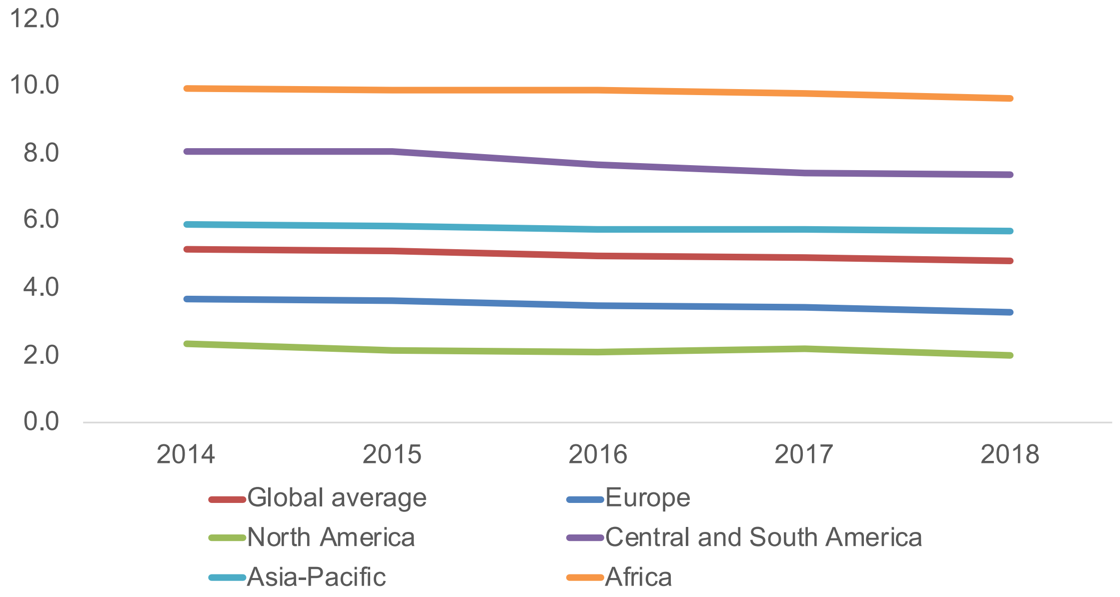


Figure 9. Money laundering/illegal activities linked to cash over GDP

Source: Author's own computation from sources described in section 4.3

The lowest estimated value of the illegal economy linked to cash is that of Switzerland (0.6% of GDP in 2018), followed by Austria (0.9%), Germany (0.9%) and Australia (1%), while the highest estimated value is observed in Nigeria (14%), followed by Thailand (13.6%) and Mexico (10.2%).

One of the most interesting observations is that the percentage of the illegal economy linked to cash has increased in countries that have traditionally maintained lower levels of cash usage. In Norway it reached 4% of GDP in 2018 and in Sweden 3.4%. Finland (2%) remains at similar levels as other more cash-incentive countries such as the United States (2%) and France (1.9%).

These results imply that the largest share of the underground economy refers to tax evaded funds that have a legal productive origin. This is illustrated in Table 10 as the difference between the estimates of the total shadow economy and the illegal economy linked to cash. Globally, it represented 15.5% of GDP in 2018, being 13.6% in Europe, 6.5% in North America, 19.4% in Central and South America, 15.2% in Asia-Pacific and 25% in Africa.

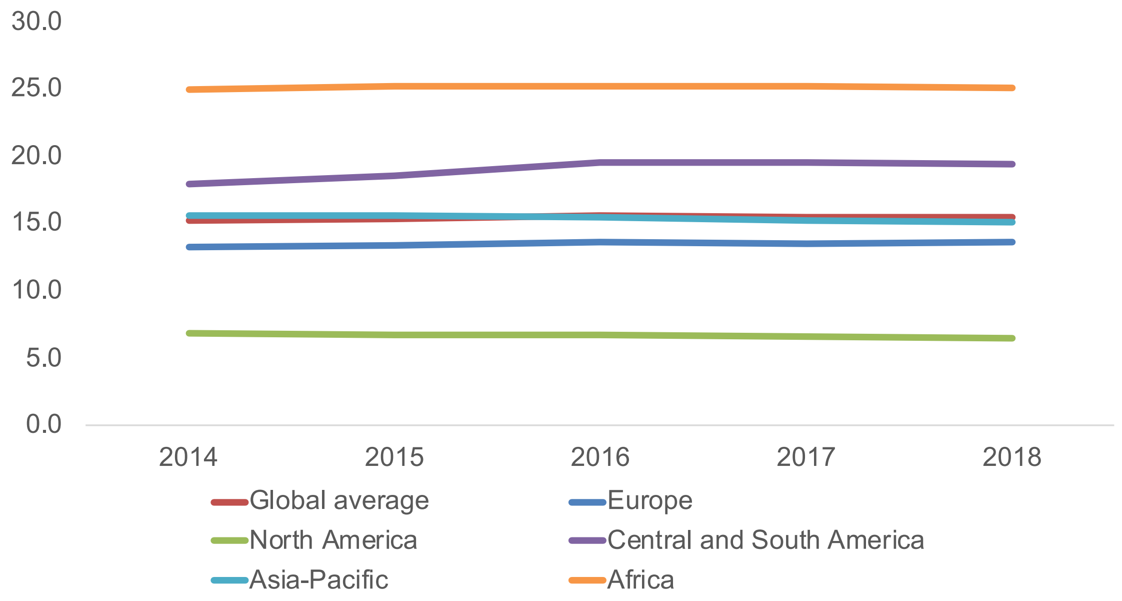


Figure 10. Shadow economy with legal origin but tax evaded

Source: Author's own computation from sources described in section 4.3

4.3.3. Card fraud

A first reference for card fraud is that related to ATMs (Figure 11). After declining sharply, coinciding with the introduction of the EMV chip, this fraud has remained steady in most geographic areas. Globally, it amounts to 14 cents of every 10,000 dollars withdrawn from an ATM. It is related to the introduction of ATM-protection techniques in different locations. Consequently, it represents 7 cents of every 1000 dollars in Europe, 23 cents in North America, 43 cents in Central and South America, 17 cents in Asia-Pacific and 18 cents in Africa.

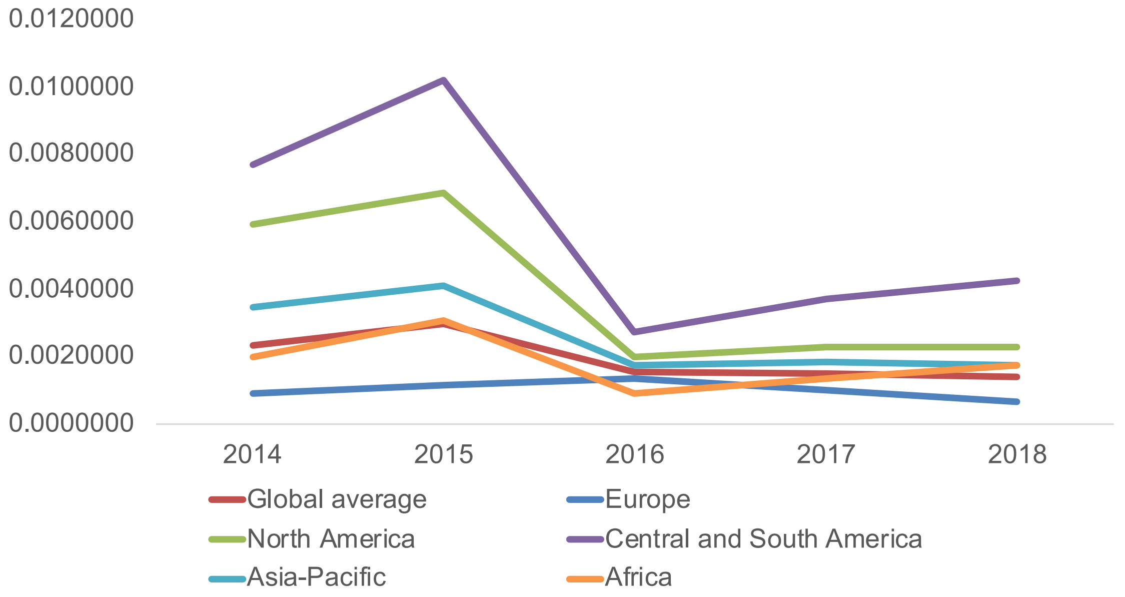


Figure 11. Card fraud: ATM lost and stolen (% of transactions)

Source: Author’s own computation from sources described in section 4.3

Card counterfeit fraud related to ATMs (Figure 12) varies significantly across geographic areas. Globally, it amounts to one dollar of every 10,000 dollars withdrawn, but it ranges from 5 cents in Europe to 4.7 in Africa, 1.4 dollars in North America, 2.8 dollars in Central and South America and 0.8 dollars in Asia-Pacific.

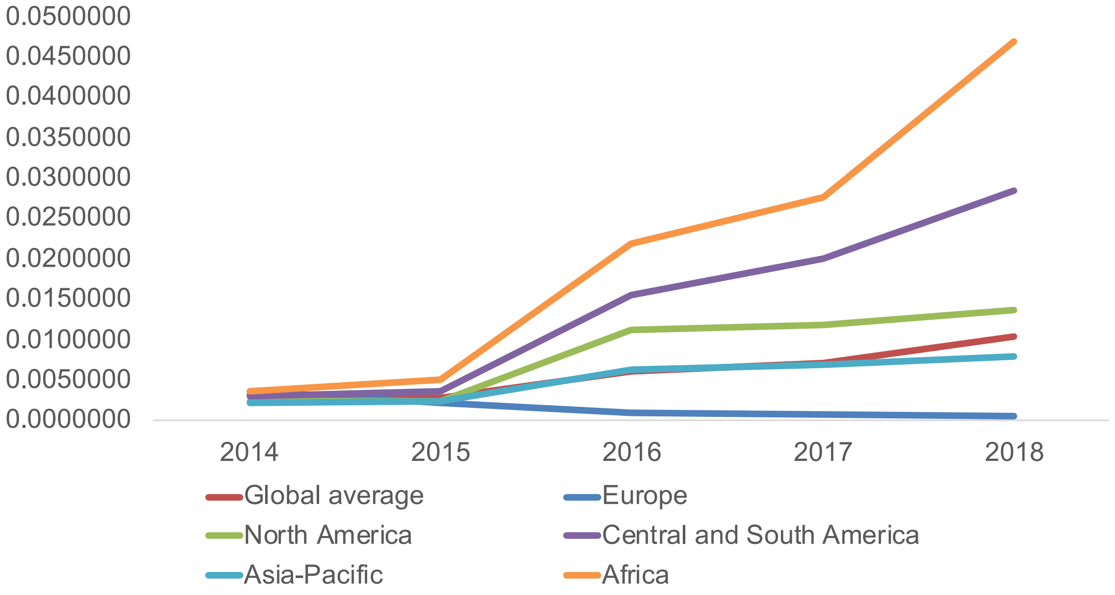


Figure 12. Card fraud: ATM counterfeit (% of transactions)

Source: Author’s own computation from sources described in section 4.3

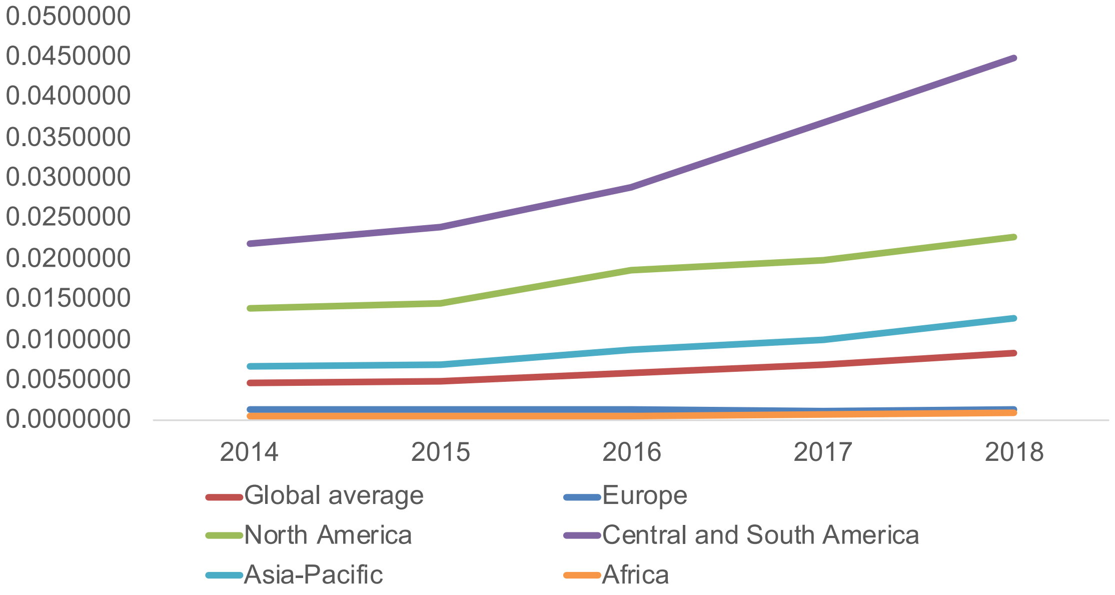


Figure 13. Card fraud: POS lost and stolen (% of transactions)

Source: Author’s own computation from sources described in section 4.3

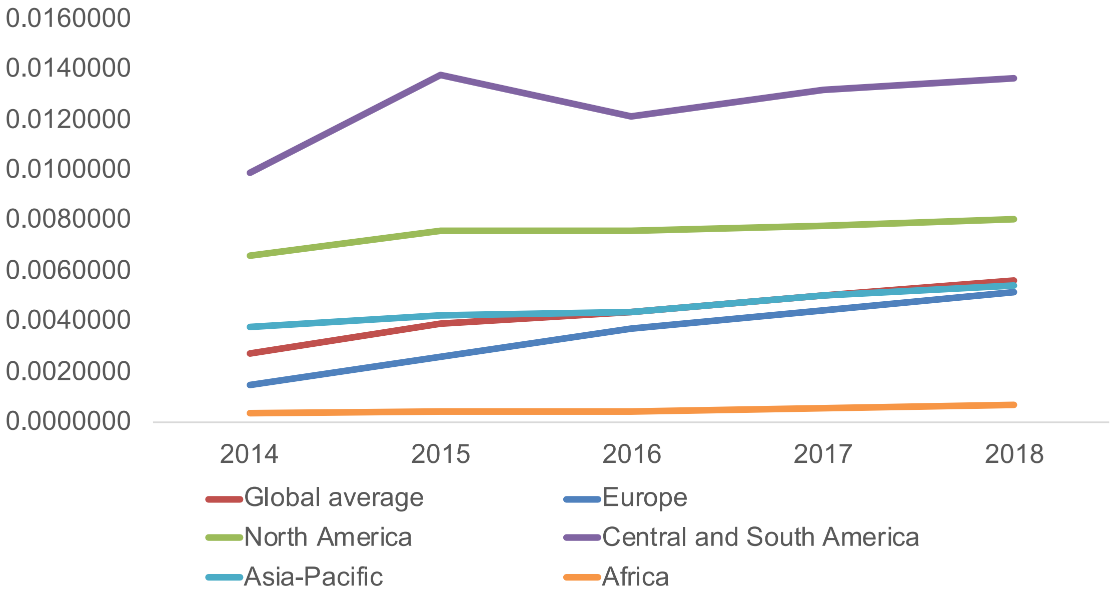


Figure 14. Card fraud: POS counterfeit (% of transactions)

Source: Author's own computation from sources described in section 4.3

As for the magnitude of card fraud committed during transactions at the point of sale, Figure 13 illustrates that lost and stolen fraud has increased over time, but particularly in some areas. Globally, this fraud represents 0.8 dollars for every 10,000 dollars in transactions. In 2018, it stood at 0.14 dollars in Europe, 2.28 in North America, 4.49 in Central and South America, 1.27 in Asia-Pacific and 0.09 in Africa.

Card counterfeit fraud at POS (Figure 14) was 56 cents for every 10,000 dollars globally in 2018. It has increased particularly in Central and South America (1.4/1000 dollars in 2018) and was 51 cents in Europe, 81 cents in North America, 55 cents in Asia-Pacific and 7 cents in Africa.

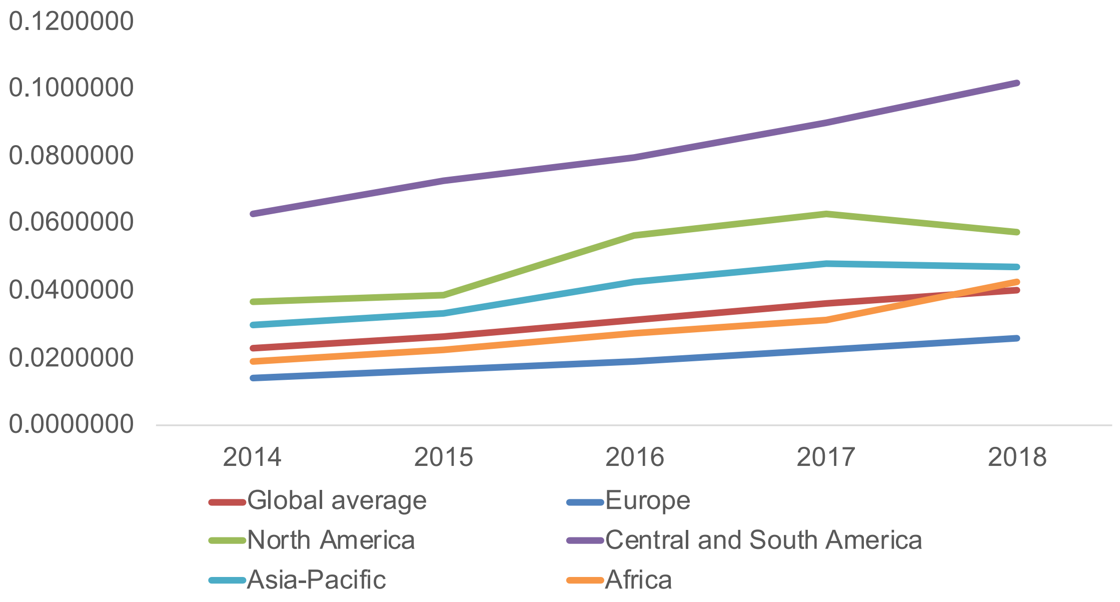


Figure 15. Card fraud: Card-not-present (CPN) (% of transactions)

Source: Author’s own computation from sources described in section 4.3

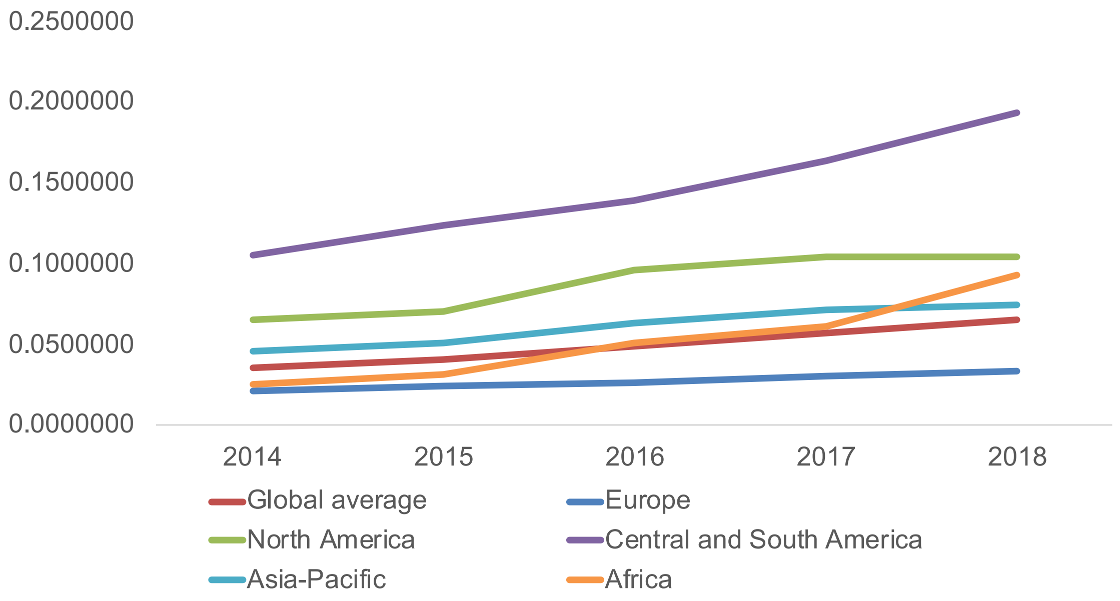


Figure 16. Total card fraud per transaction (%)

Source: Author’s own computation from sources described in section 4.3

In any event, the largest proportion of card fraud is represented by card-not-present fraud, which has been growing constantly in all the geographic areas considered (Figure 15). It represents 4 dollars of every 10,000 dollars in card POS transactions globally. The numbers range from 2.6 dollars in Europe to 10.2 dollars in Central and South America, 5.7 dollars in North America, 4.7 dollars in Asia-Pacific and 4.3 dollars in Africa.

The sum of all the categories of card fraud reveals total card fraud in 2018 of 6 cents per every 100 dollars and it has been increasing in all locations between 2014 and 2018 (Figure 16). In 2018, it amounted to 3.4 cents in Europe, 10.4 cents in North America, 19.3 cents in Central and South America, 7.5 cents in Asia-Pacific and 9.3 cents in Africa. As illustrated in Table 2, CNP fraud constitutes more than half of total card fraud.

Table 2. Composition of card fraud (% of total fraud)

	ATM LOST AND STOLEN	ATM COUNTERFEIT	POS LOST AND STOLEN	POS COUNTERFEIT	CNP FRAUD
Global average	4.91	9.82	15.50	11.57	58.19
Europe	4.93	7.49	5.44	12.20	69.94
North America	5.49	7.77	20.80	13.51	52.43
Central and South America	4.82	7.41	22.23	14.90	50.63
Asia-Pacific	5.29	7.36	15.30	11.45	60.61
Africa	4.08	26.93	22.22	1.25	45.51

Source: Author's own computation from sources described in section 4.3

The average value for each one of the indicators analysed for 2014–2018 is presented in Table 3.

Table 3. Average value of the main fraud and related indicators for 2014–2018

	Global average	Europe	North America	Central and South America	Asia-Pacific	Africa
ATM LOST AND STOLEN (% per transaction)	0.0021	0.0011	0.0043	0.0061	0.0028	0.0018
ATM COUNTERFEIT (% per transaction)	0.0042	0.0017	0.0060	0.0093	0.0039	0.0120
POS LOST AND STOLEN (% per transaction)	0.0066	0.0012	0.0161	0.0280	0.0081	0.0099
POS COUNTERFEIT (% per transaction)	0.0049	0.0027	0.0105	0.0188	0.0060	0.0006
CNP FRAUD (% per transaction)	0.0246	0.0157	0.0406	0.0638	0.0319	0.0203
CARD FRAUD PER TRANSACTION	0.0423	0.0224	0.0775	0.1260	0.0527	0.0446
DEMAND FOR CASH (%)	11.22	12.77	7.07	14.08	7.43	8.24
CASH DEPOSITS/ TOTAL DEPOSITS (%)	48.65	62.55	18.58	24.18	26.27	43.19
SHADOW ECONOMY / GDP (%)	20.42	17.00	8.88	26.67	21.20	34.96
MONEY LAUNDERING/ ILLEGAL ECONOMY LINKED TO CASH (%)	4.99	3.51	2.17	7.72	5.79	9.83
SHADOW ECONOMY WITH LEGAL ORIGIN BUT TAX EVADED (%)	15.4	13.5	6.7	19.0	15.4	25.1

Source: Author’s own computation from sources described in section 4.3

4.3.4 Comparative trends

Table 4 presents the ratio of the value of each indicator in 2018 over the value in 2014, for the global average and each of the five geographic areas. The main conclusions are the following:

- The illegal economy linked to cash in 2018 was 0.93 times the value of 2014. However, total card fraud per transaction almost doubled (1.82).

- Fraud with cash has been decreasing 1.7% annually while fraud with cards have been increasing 16.2% annually. Since 2014, fraud with cash decreases and fraud with cards increases.

- While the total shadow economy remained relatively stable during the period (ratio 2018/2014 = 0.99) the illegal economy linked to cash shrunk (0.93). This happens despite a general increased in the demand for cash (1.18) and on the ratio of transferable deposits over total deposits (1.20).

- The card-not-present (CNP) fraud grew more than any other type of fraud. It was 6.44 times larger in 2018 than in 2014. The introduction of the EMV chip in many jurisdictions have reduced the card lost and stolen fraud but increased more than proportionally the CNP fraud.

- ATM-related card counterfeit also increased during the period (2.23) while POS counterfeit declined (0.61).

Table 4. Change in the main magnitudes of fraud and other related indicators (ratio 2018/2014)

	Global average	Europe	North America	Central and South America	Asia-Pacific	Africa
ATM LOST AND STOLEN	0.64	1.11	0.38	0.48	0.53	0.67
ATM COUNTERFEIT	2.23	0.22	5.08	6.38	3.19	7.74
POS LOST AND STOLEN	0.67	2.72	1.45	1.30	1.27	0.02
POS COUNTERFEIT	0.61	3.09	0.34	0.29	0.39	0.63
CNP FRAUD	6.44	4.43	7.83	6.61	8.83	44.16
CARD FRAUD PER TRANSACTION	1.82	1.57	1.59	1.82	1.63	3.64
DEMAND FOR CASH	1.18	1.37	1.05	0.77	0.98	0.86
TRANSFERABLE DEPOSITS/ TOTAL DEPOSITS	1.20	1.26	1.36	0.91	1.09	1.03
SHADOW ECONOMY / GDP	0.99	0.99	0.92	1.03	0.97	0.99
MONEY LAUNDERING/ ILLEGAL ECONOMY LINKED TO CASH	0.93	0.89	0.85	0.91	0.97	0.97
SHADOW ECONOMY WITH LEGAL ORIGIN BUT TAX EVADED	1.01	1.02	0.94	1.08	0.97	1.00

Source: Author's own computation from sources described in section 4.3

5. Projections on the size of cash versus electronic card fraud based on the projected international structure of payment means

This section offers some projections on the main magnitudes of this study, in particular, card fraud per transaction and the illegal economy linked to cash as a percentage of GDP. It also includes the demand for cash as a main reference for other estimations. The projections are obtained by applying projections of the main explanatory variables of equations (1) and (2) to the estimated coefficients of the two models presented in Appendix A. The trend of the main variables over the five years is applied to estimate their value in 2025. Therefore, this long-term projection assumes that the values in 2025 will result from maintaining, from 2019 to 2025, the same trends observed from 2014 to 2018. Though imperfect, they serve as a reference for policy orientation and to explore how fraud will evolve if the current conditions are maintained.

Table 5. Change in the main magnitudes of fraud and other related indicators (ratio 2018/2014)

	Year	Global average	Europe	North America	Central and South America	Asia-Pacific	Africa
CARD FRAUD PER TRANSACTION (%)	2018	0.066	0.034	0.104	0.193	0.075	0.093
	2025(P)	0.139	0.076	0.194	0.388	0.150	0.189
MONEY LAUNDERING/ ILLEGAL ECONOMY LINKED TO CASH	2018	4.8	3.3	2.0	7.4	5.7	9.6
	2025(P)	4.3	2.9	1.8	7.2	5.0	9.1
DEMAND FOR CASH (%)	2018	11.9	14.1	7.1	13.1	7.6	7.9
	2025(P)	11.7	14.0	7.0	12.9	7.0	7.4

Source: Author's own computation from sources described in section 4.3

The main results are as follows:

- If the current trends hold, card fraud per transaction is expected to double by 2025;
- The illegal economy linked to cash would fall by 10.4% (to 4.3% of GDP in 2025); and
- The demand for cash will only fall by 1.7% from 2018 to 2025 and the ratio of currency in circulation to broad money would be 11.7% in 2025.

6. Conclusions

Battling fraud in payment instruments is a combined effort of public authorities and private stakeholders. While technological innovations have provided new tools to prevent and detect fraud, they have also offered a wide range of possibilities for fraudsters to exploit gaps and failures attached to devices, software and communications. Social engineering has become more sophisticated with cybercrime and represents a policy challenge throughout the world.

This report offers two main contributions. First of all, it provides a comprehensive taxonomy of payment fraud alternatives related to both cash and electronic payments. Second, it offers an empirical estimation of the value of fraud with different cash and card payments, as well as some insights into the impact of new forms of electronic transactions, such as contactless payments and cryptocurrencies. The empirical analysis was conducted for the period 2014–2018 for 52 countries in Europe, North America, Central and South America, Asia-Pacific and Africa. In addition, the report provides some projections on what fraud will look like by 2025.

The main conclusions of the study are the following:

i) Fraud does not constitute an intrinsic characteristic of payment instruments, but is a social problem that needs to be addressed with the appropriate public policies and private efforts. The empirical evidence of the report indicates that, as other electronic payment instruments have been growing alongside cash, a significant share of fraud has moved from cash to electronic means of payment.

ii) As technology evolves, there is a diversification of payment channels and options. This has been particularly acute in the aftermath of the crisis, when social engineering has emerged as a substantial public policy problem. While technology improves security in certain segments, other opportunities for fraud emerge. This has been the case with the EMV chip in payment cards. As the EMV chip has been implemented in many countries, a transfer from 'lost and stolen' or 'counterfeit' fraud to card-not-present fraud has been observed.

iii) There is a need to distinguish fraud related to tax evasion but derived from activities with a legal productive origin from fraud attached to illegal and non-productive activities. Importantly, the empirical evidence in this report indicates that cash related to illegal activities represents less than one fourth of the underground economy and this figure has been falling recently. However, other forms of fraud such as CNP have increased by more than six times between 2014 and 2018 alone. Fraud with cash has been decreasing 1.7% annually while fraud with cards have been increasing 16.2% annually. Since 2014, fraud with cash decreases and fraud with cards increases.

iv) The faster growth of card fraud compared to cash fraud has been compatible with a high demand for cash during a period of low interest rates in many jurisdictions. As demonstrated in the report, this persistence of demand for cash has increased the structural (legal) component of the demand for currency.

v) If the current trends persist, card fraud per transaction would double by 2025, while the illegal economy linked to cash would fall by 10.4%.

References

ACI Worldwide (2019), Global Cross-Channel Payment Fraud Increases 13 Percent During 2018 Peak Holiday Season (Jan 15, 2019) https://www.aciworldwide.com/news-and-events/press-releases/2019/january/global-cross-channel-payment-fraud-increases-13-percent-during-2018-peak-holiday-season

Aeorospike (2019), Enabling Digital Payments Transformation. Aerospike INC. https://aero-media.aerospike.com/2018/08/Enabling-Digital-Payments-Transformation-solution-brief.pdf

Ainsworth, R.T. (2016) Sales suppression: the international dimension. American University Law Review. 65, 1241-1270.

Ainsworth, R.T. (2019) Zappers & Phantom-Ware: A Global Demand for Tax Fraud Technology.
50 Tax Notes International 1017. Boston Univ. School of Law Working Paper No. 08-20 (revised Dec 2019).

Aite (2016). 2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From. https://aitegroup.com/report/2016-global-consumer-card-fraud-where-card-fraud-coming

Ardizzi, G., Petraglia, C., Piacenza, M., & Turati, G. (2014a). Measuring the underground economy with the currency demand approach: A reinterpretation of the methodology, with an application to Italy. Review of Income and Wealth, 60(1), 747–772.

Ardizzi, G., Petraglia, C., Piacenza, M., Schneider, F., Turati, G., (2014b). Money laundering as a crime in the financial Sector: a new approach to quantitative assessment, with an application to Italy. J. Money Credit Bank. 46 (8),1555–1590.

Australian Payments Network Fraud Statistics (2014 to 2018) https://www.auspaynet.com.au/sites/default/files/2019-08/AustralianPaymentCardFraud2019_0.pdf

Board of Governors of the Federal Reserve System (2014-2018). Networks, Processors, and Issuers Payments Surveys (NPIPS).

Ciphertrace (2020), Cryptocurrency Anti-Money Laundering Report, 2019 Q4. https://ciphertrace.com/crypto-aml-report-2018q3.pdf

ConsumerProtect (2018). 11 Common Types Of Credit Card Scams & Fraud. https://www.consumerprotect.com/crime-fraud/11-types-of-credit-card-fraud-scams/

Crowe LLP (2019), The financial cost of fraud report 2018, https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/Financial-Cost-of-Fraud-2018.ashx?la=en-GB&hash=F3D9DED968C59B2469729C7FDCDDFF9B481C65BC

Equifax (2018), Guide to avoiding contactless card fraud, https://www.equifax.co.uk/resources/identity_protection/how-to-avoid-contactless-card-fraud.html

European Association of Secure Transactions (2019), Terminal fraud definitions & terminology (ATM, UPT & POS). https://www.association-secure-transactions.eu/files/EAST-Terminal-Fraud-Definitions-Terminology-ATM-UPT-POS.pdf

European Central Bank (2014-2018) Card Fraud Report.

European Payments Council (2019), Payment threats and fraud trends report, December 2019 https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

Federal Bureau of Investigation. (2011) “Financial Crimes Report to the Public.” http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010--2011/financialcrimes-report-2010--2011#Asset.

Federal Bureau of Investigation. (2019), Internet Crime Report 2019, https://pdf.ic3.gov/2019_IC3Report.pdf

Fischer, B., Koehler, P. and F. Seitz (2004). The Demand for Euro Area Currencies: Past, Present and Future. ECB Working Paper No. 330

Houben, R. and A. Snyers (2018), Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion. EU Directorate-General for Internal Policies. PE 619.024 - July 2018. https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1

Juniper Research (2019), POS & mPOS Terminals: Vendor Strategies, Positioning & Market Forecasts 2017-2022. https://www.juniperresearch.com/researchstore/fintech-payments/pos-hardware-and-software-research-report

Juniper Research (2020), Online Payment Fraud White Paper 2016-2020 https://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-payment-fraud-wp-2016.pdf

Katarzyna, C. (2019) Cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems. 2019 OECD Global Anti-Corruption & Integrity Forum http://www.oecd.org/corruption/integrity-forum/academic-papers/Ciupa-Katarzyna-cryptocurrencies.pdf

KPMG (2019). Global Banking Fraud Survey, May 2019. https://home.kpmg/xx/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html

LexisNexis (2015), The True Cost of Fraud: Merchants Contend with Increasing Fraud Losses as Remote Channels Prove Especially Challenging. https://www.lexisnexis.com/risk/downloads/assets/true-cost-of-fraud-2015-study.pdf

LexisNexis (2019), Online Payment Fraud Trends: 8 Predictions for 2019.

Nets (2019), European Fraud Report – Payments Industry Challenges. https://www.nets.eu/solutions/fraud-and-dispute-services/Documents/Nets-Fraud-Report-2019.pdf

Nilson (2019), The Nilson Report. Issue 1164, nov 2019 https://nilsonreport.com/mention/407/1link/

OECD (2013). Electronic sales suppression: a threat to tax revenues, https://www.oecd.org/ctp/crime/ElectronicSalesSupression.pdf

Proofpoint (2019), Proofpoint Annual Human Factor Report. https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more

Schneider, F. (2002). The Shadow Economy: Theoretical Approaches, Empirical Studies, and Political Implications, Cambridge University Press, Cambridge, 2002.

Schneider, F. (2007). Shadow economies and corruption all over the world: New estimates for 145 countries. Economics: The Open-Access, Open-Assessment E-Journal No. 2007-9.

Schneider, F. (2010). Turnover of Organized Crime and Money Laundering: Some Preliminary Empirical Findings, Public Choice, 144, 473–86.

Schneider, F. (2011). Handbook on the Shadow Economy, Edward Elgar, Cheltenham.

Sullivan, R. J. (2010), "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options", Federal Reserve Bank of Kansas City, Economic Review • second quarter 2010, 101-133.

The Economist. (2018, April 26). Crypto money-laundering. https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering

APPENDIX A. ESTIMATED EQUATIONS

A1. Estimated coefficients of the equation measuring the demand for cash. 52 countries. 2015-2018

Dependent variable: currency in circulation/broad money								
	(I)		(II)		(III)		(IV)	
STRUCTURAL								
Per capita GDP	-0.0218	***	-		-0.0195	***	-0.0207	***
	(-2.94)				(-2.87)		(-3.06)	
Unemployment rate	0.2328	***	0.259	***	-		0.2593	***
	(-3.49)		(-3.63)				(-3.31)	
Transferable deposits/total bank deposits	0.3605	**	0.3108	**	0.3416	*	0.3792	*
	(-2.16)		(-2.11)		(-1.90)		(-1.85)	
POS transactions to GDP	-0.0805	***	-0.0729	***	-0.0701	***	-0.0774	***
	(-4.21)		(-4.03)		(-4.82)		(-4.30)	
Interest rate on bank deposits	-0.0006	*	-0.0009	*	-0.0007	*	-	
	(-1.93)		(-1.99)		(-2.12)			
UNDERGROUND								
Tax burden	0.0399	***	0.0361	***	0.4092	***	0.0409	***
	(-4.68)		(-4.89)		(-4.36)		(-4.29)	
Employment in agriculture	0.3811	***	0.3508	***	0.3693	***	0.343	***
	(-3.52)		(-3.68)		(-3.49)		(-3.75)	
Employment in construction	0.2243	***	0.2629	***	0.2433	***	0.2191	***
	(-3.09)		(-3.22)		(-3.01)		(-3.17)	
ILLEGAL								
Crime	0.085	***	0.0814	***	0.0815	***	0.0874	***
	(-2.86)		(-3.02)		(-2.94)		(-2.98)	
Constant	0.1639	***	0.1419	***	0.1773	***	0.1563	***
	(-5.13)		(-5.37)		(-4.98)		(-4.55)	
Observations	260		260		260		260	
Wald test	2638.29		3903.56		3115.29		2907.08	
Pseudo R2	0.91		0.89		0.9		0.88	
Country effects	Yes		Yes		Yes		Yes	
Year effects	Yes		Yes		Yes		Yes	
t-statistics in parentheses								
***,**,*: Statistically significant at 1%, 5%, 1%, respectively								

A2. Estimated coefficients of the equation calibrating card fraud per transaction. 52 countries. 2015-2018

Dependent variables: card fraud per transaction (I), ATM fraud (II), CNP fraud (III)						
	(I)		(II)		(III)	
ATM transaction size	0.0962	**	0.1125	*	-0.0163	
	(-2.21)		(-1.94)		(-0.35)	
ATMs per inhabitant	0.1059	***	0.1233	***	0.0259	
	(-4.19)		(-3.81)		(-0.72)	
POS transaction size	0.1153	**	0.0562	**	0.2983	***
	(-2.16)		(-2.29)		(-4.49)	
POS devices per inhabitant	0.0933	**	0.0521		0.1309	***
	(-2.26)		(-0.64)		(-2.87)	
Burglary	0.0941	***	0.0435	**	0.1113	***
	(-5.24)		(-2.23)		(-5.03)	
Theft	0.193	***	0.2988	***	0.2633	***
	(-6.02)		(-5.74)		(-4.88)	
Employment in the retail commercial sector	0.0016	*	0.0035	***	0.0795	***
	(-1.93)		(-3.02)		(-3.88)	
Employment in tourism	0.3795	***	0.4126	***	0.443	***
	(-4.43)		(-3.40)		(-4.19)	
EMV chip adopted	0.0826		-0.0962	**	0.0994	***
	(-0.79)		(-2.13)		(-3.96)	
Constant	0.1937	***	0.2349	***	0.6332	***
	(-4.77)		(-2.93)		(-5.31)	
Observations	260		260		260	
Wald test	1909.61		2325.6		2934	
Pseudo R2	0.76		0.78		0.79	
Country effects	Yes		Yes		Yes	
Year effects	Yes		Yes		Yes	
t-statistics in parentheses						
***,**,*: Statistically significant at 1%, 5%, 1%, respectively						

APPENDIX B. MAIN FIGURES BY COUNTRY

A1. ATM LOST AND STOLEN (% PER TRANSACTION)					
	2014	2015	2016	2017	2018
Austria	0.000200	0.000150	0.000100	0.000074	0.000048
Belgium	0.002300	0.003150	0.004000	0.002960	0.001920
Bulgaria	0.000200	0.000100	0.000000	0.000000	0.000000
Croatia	0.000200	0.004600	0.009000	0.006660	0.004320
Cyprus	0.000400	0.000200	0.000000	0.000000	0.000000
Czech Republic	0.000200	0.000150	0.000100	0.000074	0.000048
Denmark	0.000800	0.004450	0.008100	0.005994	0.003888
Estonia	0.000100	0.000050	0.000000	0.000000	0.000000
Finland	0.001300	0.001250	0.001200	0.000888	0.000576
France	0.006900	0.006400	0.005900	0.004366	0.002832
Germany	0.002400	0.002250	0.002100	0.001554	0.001008
Greece	0.000000	0.000000	0.000000	0.000000	0.000000
Hungary	0.000300	0.000200	0.000100	0.000074	0.000048
Ireland	0.000600	0.000550	0.000500	0.000370	0.000240
Italy	0.001000	0.000950	0.000900	0.000666	0.000432
Latvia	0.000000	0.000000	0.000000	0.000000	0.000000
Lithuania	0.000000	0.000000	0.000000	0.000000	0.000000
Luxemburg	0.001500	0.001300	0.001100	0.000814	0.000528
Malta	0.000900	0.000950	0.001000	0.000740	0.000480
Netherlands	0.002000	0.001300	0.000600	0.000444	0.000288
Poland	0.000200	0.000200	0.000200	0.000148	0.000096
Portugal	0.000400	0.000300	0.000200	0.000148	0.000096
Romania	0.000000	0.000000	0.000000	0.000000	0.000000
Slovakia	0.000100	0.000050	0.000000	0.000000	0.000000
Slovenia	0.000200	0.000150	0.000100	0.000074	0.000048
Spain	0.000900	0.000950	0.001000	0.000740	0.000480
Sweden	0.001100	0.001150	0.001200	0.000888	0.000576
United Kingdom	0.000800	0.000700	0.000600	0.000444	0.000288
Switzerland	0.001071	0.001350	0.001629	0.001205	0.000782
Norway	0.001210	0.001265	0.001320	0.000977	0.000634
United States	0.006480	0.007470	0.002160	0.002490	0.002490
Canada	0.005378	0.006200	0.001793	0.002067	0.002067
Brazil	0.011016	0.013446	0.003456	0.004731	0.004980
Mexico	0.013608	0.016434	0.004320	0.005727	0.005976
Colombia	0.004957	0.007530	0.002056	0.002839	0.003573
Chile	0.004561	0.006875	0.001906	0.002646	0.003495
Argentina	0.004357	0.006641	0.001849	0.002563	0.003244
Australia	0.000148	0.000153	0.000161	0.000186	0.000196

Japan	0.008144	0.010432	0.002916	0.003386	0.003436
India	0.007330	0.009597	0.002712	0.003115	0.003058
China	0.000804	0.000500	0.000497	0.000656	0.000812
Malaysia	0.000764	0.000480	0.000483	0.000646	0.000777
Thailand	0.001890	0.002090	0.002300	0.001717	0.001123
Hong Kong	0.002079	0.002508	0.003220	0.002232	0.001348
South Korea	0.000886	0.000556	0.000559	0.000743	0.000949
Russia	0.009019	0.010781	0.002895	0.003722	0.003851
South Africa	0.000117	0.000122	0.000131	0.000135	0.000138
Nigeria	0.003922	0.005977	0.001664	0.002307	0.002920
Egypt	0.003385	0.005266	0.001486	0.002074	0.002637
Morocco	0.001693	0.002633	0.000743	0.001037	0.001318
Zambia	0.001442	0.002259	0.000697	0.001240	0.001830
Mozambique	0.001356	0.002169	0.000676	0.001166	0.001702
Global average	0.002320	0.002966	0.001531	0.001495	0.001376
Europe	0.000909	0.001137	0.001365	0.001010	0.000655
North America	0.005929	0.006835	0.001976	0.002278	0.002278
Central and South America	0.007700	0.010185	0.002717	0.003701	0.004254
Asia-Pacific	0.003451	0.004122	0.001749	0.001823	0.001728
Africa	0.001986	0.003071	0.000899	0.001326	0.001757

A2. ATM COUNTERFEIT (% PER TRANSACTION)

	2014	2015	2016	2017	2018
Austria	0.006300	0.003950	0.001600	0.001184	0.000768
Belgium	0.001700	0.001350	0.001000	0.000740	0.000480
Bulgaria	0.002000	0.001650	0.001300	0.000962	0.000624
Croatia	0.001200	0.000800	0.000400	0.000296	0.000192
Cyprus	0.005200	0.003200	0.001200	0.000888	0.000576
Czech Republic	0.002500	0.001350	0.000200	0.000148	0.000096
Denmark	0.006600	0.004050	0.001500	0.001110	0.000720
Estonia	0.005100	0.002900	0.000700	0.000518	0.000336
Finland	0.002800	0.003300	0.003800	0.002812	0.001824
France	0.004800	0.003300	0.001800	0.001332	0.000864
Germany	0.006700	0.004400	0.002100	0.001554	0.001008
Greece	0.000100	0.000050	0.000000	0.000000	0.000000
Hungary	0.000800	0.000500	0.000200	0.000148	0.000096
Ireland	0.003400	0.002550	0.001700	0.001258	0.000816
Italy	0.001100	0.000800	0.000500	0.000370	0.000240
Latvia	0.005400	0.003050	0.000700	0.000518	0.000336
Lithuania	0.001400	0.000800	0.000200	0.000148	0.000096
Luxemburg	0.006600	0.003550	0.000500	0.000370	0.000240
Malta	0.006400	0.003500	0.000600	0.000444	0.000288
Netherlands	0.014900	0.008100	0.001300	0.000962	0.000624
Poland	0.001700	0.001000	0.000300	0.000222	0.000144
Portugal	0.001400	0.001000	0.000600	0.000444	0.000288
Romania	0.000500	0.000250	0.000000	0.000000	0.000000
Slovakia	0.000900	0.000650	0.000400	0.000296	0.000192
Slovenia	0.002100	0.001600	0.001100	0.000814	0.000528
Spain	0.001000	0.000800	0.000600	0.000444	0.000288
Sweden	0.003800	0.003100	0.002400	0.001776	0.001152
United Kingdom	0.002400	0.001800	0.001200	0.000888	0.000576
Switzerland	0.004234	0.002715	0.001196	0.000885	0.000574
Norway	0.004180	0.003410	0.002640	0.001954	0.001267
United States	0.002550	0.002640	0.012240	0.012960	0.014940
Canada	0.002117	0.002191	0.010159	0.010757	0.012400
Brazil	0.004335	0.004752	0.019584	0.024624	0.032868
Mexico	0.005355	0.005808	0.024480	0.029808	0.035856
Colombia	0.002124	0.002922	0.011980	0.016006	0.025366
Chile	0.001954	0.002668	0.011105	0.014917	0.024808
Argentina	0.001867	0.002578	0.010770	0.014453	0.023032
Australia	0.000295	0.000305	0.000323	0.000371	0.000392
Japan	0.002916	0.003355	0.015037	0.016039	0.018762
India	0.002625	0.003086	0.013984	0.014756	0.016698

China	0.001756	0.002126	0.002512	0.002756	0.002865
Malaysia	0.001860	0.002276	0.002717	0.003028	0.003054
Thailand	0.002020	0.001624	0.001236	0.000928	0.000622
Hong Kong	0.002222	0.001819	0.001421	0.001060	0.000706
South Korea	0.002129	0.002601	0.003107	0.003436	0.003680
Russia	0.003549	0.003810	0.016404	0.019373	0.024643
South Africa	0.000195	0.000204	0.000237	0.000281	0.000311
Nigeria	0.003361	0.004640	0.019386	0.026016	0.041458
Egypt	0.003065	0.004274	0.018036	0.024446	0.039346
Morocco	0.001533	0.002137	0.009018	0.012223	0.019673
Zambia	0.006682	0.009787	0.042023	0.051776	0.091441
Mozambique	0.006595	0.009866	0.042800	0.051103	0.089292
Global average	0.003237	0.002787	0.006160	0.007204	0.010335
Europe	0.003574	0.002316	0.001058	0.000783	0.000508
North America	0.002333	0.002416	0.011200	0.011858	0.013670
Central and South America	0.003127	0.003746	0.015584	0.019962	0.028386
Asia-Pacific	0.002152	0.002334	0.006305	0.006861	0.007936
Africa	0.003572	0.005151	0.021917	0.027641	0.046920

A3. POS LOST AND STOLEN (% PER TRANSACTION)

	2014	2015	2016	2017	2018
Austria	0.002700	0.002150	0.001600	0.001584	0.001568
Belgium	0.001200	0.001000	0.000800	0.000792	0.000784
Bulgaria	0.000100	0.000100	0.000100	0.000099	0.000098
Croatia	0.001000	0.000800	0.000600	0.000594	0.000588
Cyprus	0.001200	0.000900	0.000600	0.000594	0.000588
Czech Republic	0.000200	0.000200	0.000200	0.000200	0.000200
Denmark	0.001700	0.002500	0.003300	0.003400	0.003500
Estonia	0.000200	0.000100	0.000000	0.000050	0.000100
Finland	0.000500	0.002150	0.003800	0.004450	0.005100
France	0.011300	0.009550	0.007800	0.007250	0.006700
Germany	0.001200	0.001150	0.001100	0.001050	0.001000
Greece	0.000700	0.000500	0.000300	0.000250	0.000200
Hungary	0.000100	0.000100	0.000100	0.000100	0.000100
Ireland	0.000900	0.001300	0.001700	0.002100	0.002500
Italy	0.001700	0.001550	0.001400	0.001300	0.001200
Latvia	0.000100	0.000150	0.000200	0.000200	0.000200
Lithuania	0.000000	0.000000	0.000000	0.000000	0.000000
Luxemburg	0.000600	0.000550	0.000500	0.000450	0.000400
Malta	0.000700	0.000650	0.000600	0.000550	0.000500
Netherlands	0.001300	0.000900	0.000500	0.000400	0.000300
Poland	0.000200	0.000450	0.000700	0.000800	0.000900
Portugal	0.000900	0.000600	0.000300	0.000250	0.000200
Romania	0.000100	0.000050	0.000000	0.000000	0.000000
Slovakia	0.000100	0.000100	0.000100	0.000100	0.000100
Slovenia	0.000200	0.000200	0.000200	0.000200	0.000200
Spain	0.003300	0.002800	0.002300	0.002000	0.001700
Sweden	0.001700	0.001900	0.002200	0.001900	0.002500
United Kingdom	0.005400	0.005900	0.006400	0.007000	0.007500
Switzerland	0.001684	0.001641	0.001603	0.001614	0.001660
Norway	0.001870	0.002090	0.002420	0.002090	0.002750
United States	0.015300	0.015840	0.020400	0.021600	0.024900
Canada	0.012699	0.013147	0.016932	0.017928	0.020667
Brazil	0.030600	0.030096	0.034680	0.043200	0.049800
Mexico	0.032130	0.034848	0.040800	0.049680	0.059760
Colombia	0.016830	0.019562	0.024276	0.032400	0.039840
Chile	0.015484	0.017860	0.022504	0.030197	0.038964
Argentina	0.014794	0.017254	0.021824	0.029257	0.036175
Australia	0.001181	0.001221	0.001290	0.001485	0.001568

Japan	0.013005	0.013622	0.017952	0.019872	0.027390
India	0.010404	0.012941	0.020106	0.024562	0.036319
China	0.001087	0.001123	0.001187	0.001366	0.001443
Malaysia	0.001053	0.001100	0.001175	0.001373	0.001407
Thailand	0.004158	0.003584	0.003174	0.003340	0.002873
Hong Kong	0.004241	0.003763	0.003555	0.003808	0.003419
South Korea	0.001250	0.001302	0.001418	0.001461	0.001556
Russia	0.023660	0.023678	0.028392	0.033402	0.038505
South Africa	0.000947	0.000982	0.001079	0.001310	0.001400
Nigeria	0.000830	0.000860	0.000946	0.001148	0.001227
Egypt	0.000699	0.000730	0.000842	0.001014	0.001080
Morocco	0.000350	0.000365	0.000421	0.000507	0.000540
Zambia	0.000245	0.000263	0.000337	0.000507	0.000594
Mozambique	0.000251	0.000275	0.000356	0.000519	0.000602
Global average	0.004693	0.004932	0.005867	0.006948	0.008330
Europe	0.001428	0.001401	0.001381	0.001379	0.001438
North America	0.014000	0.014494	0.018666	0.019764	0.022784
Central and South America	0.021967	0.023924	0.028817	0.036947	0.044908
Asia-Pacific	0.006671	0.006926	0.008694	0.010074	0.012720
Africa	0.000554	0.000579	0.000664	0.000834	0.000907

A4. POS COUNTERFEIT (% PER TRANSACTION)					
	2014	2015	2016	2017	2018
Austria	0.002700	0.003200	0.003700	0.003900	0.004100
Belgium	0.001200	0.003600	0.006000	0.006900	0.007800
Bulgaria	0.000100	0.003050	0.006000	0.007350	0.008700
Croatia	0.000600	0.000750	0.000900	0.000950	0.001000
Cyprus	0.001200	0.002350	0.003500	0.004200	0.004900
Czech Republic	0.000200	0.000175	0.000150	0.002075	0.004000
Denmark	0.001700	0.004750	0.007800	0.007700	0.007600
Estonia	0.000200	0.001800	0.003400	0.004650	0.005900
Finland	0.000500	0.003550	0.006600	0.006850	0.007100
France	0.004800	0.004200	0.003600	0.003500	0.003400
Germany	0.001200	0.001150	0.001100	0.001200	0.001300
Greece	0.000700	0.000950	0.001200	0.001300	0.001400
Hungary	0.000100	0.000800	0.001500	0.001700	0.001900
Ireland	0.009000	0.008250	0.007500	0.007250	0.007000
Italy	0.001700	0.001550	0.001400	0.001300	0.001200
Latvia	0.000100	0.000700	0.001300	0.001600	0.001900
Lithuania	0.000000	0.000350	0.000700	0.004850	0.009000
Luxemburg	0.000600	0.004350	0.008100	0.008850	0.009600
Malta	0.000700	0.003950	0.007200	0.007950	0.008700
Netherlands	0.001300	0.001400	0.001500	0.001650	0.001800
Poland	0.000200	0.001750	0.003300	0.004300	0.005300
Portugal	0.000900	0.005550	0.010200	0.013100	0.016000
Romania	0.000100	0.000650	0.001200	0.001450	0.001700
Slovakia	0.000100	0.000500	0.000900	0.001100	0.001300
Slovenia	0.000200	0.001550	0.002900	0.003750	0.004600
Spain	0.003300	0.003400	0.003500	0.003950	0.004400
Sweden	0.001700	0.002850	0.004000	0.005150	0.006300
United Kingdom	0.005400	0.004600	0.003800	0.003650	0.003500
Switzerland	0.001736	0.003074	0.004412	0.005236	0.006060
Norway	0.001870	0.003135	0.004400	0.005665	0.006930
United States	0.007200	0.008300	0.008300	0.008500	0.008800
Canada	0.005976	0.006889	0.006889	0.007055	0.007304
Brazil	0.012240	0.014940	0.013280	0.016150	0.017600
Mexico	0.015120	0.018260	0.016600	0.019550	0.021120
Colombia	0.007956	0.012699	0.010890	0.010659	0.010208
Chile	0.007320	0.011594	0.010095	0.009934	0.009983
Argentina	0.006993	0.011201	0.009790	0.009625	0.009269
Australia	0.000591	0.000610	0.000645	0.000742	0.000784
Japan	0.005760	0.006640	0.006640	0.007650	0.007920

India	0.005184	0.005312	0.005644	0.006044	0.006415
China	0.000543	0.000562	0.000594	0.000683	0.000721
Malaysia	0.000598	0.000674	0.000730	0.000861	0.001003
Thailand	0.005346	0.005780	0.006300	0.007110	0.007920
Hong Kong	0.005453	0.005953	0.006867	0.008177	0.009346
South Korea	0.000658	0.000764	0.000907	0.001171	0.001389
Russia	0.010021	0.011979	0.011124	0.012706	0.013608
South Africa	0.000390	0.000384	0.000390	0.000463	0.000543
Nigeria	0.000357	0.000352	0.000357	0.000424	0.000498
Egypt	0.000317	0.000316	0.000324	0.000388	0.000460
Morocco	0.000159	0.000158	0.000162	0.000194	0.000230
Zambia	0.000666	0.000726	0.000777	0.001009	0.001289
Mozambique	0.000613	0.000682	0.000738	0.000968	0.001250
Global average	0.002761	0.003898	0.004419	0.005060	0.005616
Europe	0.001470	0.002598	0.003725	0.004436	0.005146
North America	0.006588	0.007595	0.007595	0.007778	0.008052
Central and South America	0.009926	0.013739	0.012131	0.013184	0.013636
Asia-Pacific	0.003795	0.004253	0.004383	0.005016	0.005456
Africa	0.000417	0.000436	0.000458	0.000574	0.000712

A5. CARD-NOT-PRESENT (CNP) FRAUD (% PER TRANSACTION)

	2014	2015	2016	2017	2018
Austria	0.022500	0.025950	0.029400	0.033150	0.036900
Belgium	0.015700	0.020500	0.025300	0.027750	0.030200
Bulgaria	0.005400	0.008600	0.011800	0.015700	0.019600
Croatia	0.000900	0.003550	0.006200	0.008450	0.010700
Cyprus	0.013800	0.015750	0.017700	0.022300	0.026900
Czech Republic	0.004500	0.005300	0.006100	0.047050	0.088000
Denmark	0.033500	0.042800	0.052100	0.060550	0.069000
Estonia	0.005200	0.006400	0.007600	0.008950	0.010300
Finland	0.007900	0.015600	0.023300	0.031400	0.039500
France	0.035900	0.041900	0.047900	0.051450	0.055000
Germany	0.012700	0.013550	0.014400	0.015850	0.017300
Greece	0.006500	0.005800	0.005100	0.006000	0.006900
Hungary	0.002000	0.003700	0.005400	0.006250	0.007100
Ireland	0.038900	0.046850	0.054800	0.059250	0.063700
Italy	0.007900	0.009650	0.011400	0.013450	0.015500
Latvia	0.007000	0.007800	0.008600	0.008950	0.009300
Lithuania	0.002000	0.003300	0.004600	0.005450	0.006300
Luxemburg	0.039200	0.033700	0.028200	0.015575	0.002950
Malta	0.044700	0.040850	0.037000	0.037950	0.038900
Netherlands	0.011500	0.012650	0.013800	0.015250	0.016700
Poland	0.002100	0.002450	0.002800	0.003200	0.003600
Portugal	0.008400	0.008250	0.008100	0.009500	0.010900
Romania	0.002400	0.003600	0.004800	0.005550	0.006300
Slovakia	0.003200	0.004500	0.005800	0.006500	0.007200
Slovenia	0.005100	0.006150	0.007200	0.008150	0.009100
Spain	0.009300	0.012500	0.015700	0.016950	0.018200
Sweden	0.009700	0.016500	0.023300	0.026450	0.029600
United Kingdom	0.043900	0.048000	0.052100	0.060250	0.068400
Switzerland	0.017220	0.019978	0.022736	0.026883	0.031031
Norway	0.010670	0.018150	0.025630	0.029095	0.032560
United States	0.040800	0.043200	0.072985	0.085300	0.072444
Canada	0.032640	0.034560	0.039840	0.040800	0.042240
Brazil	0.081600	0.086400	0.089640	0.096900	0.105600
Mexico	0.085680	0.095040	0.099600	0.117300	0.126720
Colombia	0.053040	0.064800	0.073729	0.083445	0.096149
Chile	0.048797	0.059162	0.068347	0.077771	0.094034
Argentina	0.046622	0.057154	0.066282	0.075351	0.087303

Australia	0.027315	0.028231	0.029841	0.034336	0.036260
Japan	0.028560	0.032400	0.062037	0.073358	0.062302
India	0.038000	0.038200	0.039500	0.040200	0.042900
China	0.021900	0.023100	0.026500	0.031589	0.033359
Malaysia	0.021243	0.022638	0.026118	0.031437	0.033142
Thailand	0.014880	0.021250	0.026690	0.030510	0.032760
Hong Kong	0.016368	0.025500	0.032562	0.038443	0.041933
South Korea	0.037202	0.044067	0.056771	0.059687	0.049015
Russia	0.063093	0.066804	0.083827	0.093918	0.091775
South Africa	0.016198	0.018011	0.024648	0.031486	0.033577
Nigeria	0.033751	0.038142	0.043630	0.047197	0.064758
Egypt	0.030714	0.035090	0.041012	0.044837	0.062168
Morocco	0.015357	0.017545	0.020506	0.022418	0.031084
Zambia	0.009214	0.014036	0.018455	0.021522	0.032327
Mozambique	0.008753	0.013054	0.017902	0.021091	0.031810
Global average	0.023104	0.026590	0.031525	0.036195	0.040217
Europe	0.014323	0.016809	0.019296	0.022775	0.026255
North America	0.036720	0.038880	0.056413	0.063050	0.057342
Central and South America	0.063148	0.072511	0.079520	0.090154	0.101961
Asia-Pacific	0.029840	0.033577	0.042650	0.048164	0.047050
Africa	0.018998	0.022646	0.027692	0.031425	0.042621

A6. CARD FRAUD (% PER TRANSACTION)					
	2014	2015	2016	2017	2018
Austria	0.034400	0.035400	0.036400	0.039892	0.043384
Belgium	0.022100	0.029600	0.037100	0.039142	0.041184
Bulgaria	0.007800	0.013500	0.019200	0.024111	0.029022
Croatia	0.003900	0.010500	0.017100	0.016950	0.016800
Cyprus	0.021800	0.022400	0.023000	0.027982	0.032964
Czech Republic	0.007600	0.007175	0.006750	0.049547	0.092344
Denmark	0.044300	0.058550	0.072800	0.078754	0.084708
Estonia	0.010800	0.011250	0.011700	0.014168	0.016636
Finland	0.013000	0.025850	0.038700	0.046400	0.054100
France	0.063700	0.065350	0.067000	0.067898	0.068796
Germany	0.024200	0.022500	0.020800	0.021208	0.021616
Greece	0.008000	0.007300	0.006600	0.007550	0.008500
Hungary	0.003300	0.005300	0.007300	0.008272	0.009244
Ireland	0.052800	0.059500	0.066200	0.070228	0.074256
Italy	0.013400	0.014500	0.015600	0.017086	0.018572
Latvia	0.012600	0.011700	0.010800	0.011268	0.011736
Lithuania	0.003400	0.004450	0.005500	0.010448	0.015396
Luxemburg	0.048500	0.043450	0.038400	0.026059	0.013718
Malta	0.053400	0.049900	0.046400	0.047634	0.048868
Netherlands	0.031000	0.024350	0.017700	0.018706	0.019712
Poland	0.004400	0.005850	0.007300	0.008670	0.010040
Portugal	0.012000	0.015700	0.019400	0.023442	0.027484
Romania	0.003100	0.004550	0.006000	0.007000	0.008000
Slovakia	0.004400	0.005800	0.007200	0.007996	0.008792
Slovenia	0.007800	0.009650	0.011500	0.012988	0.014476
Spain	0.017800	0.020450	0.023100	0.024084	0.025068
Sweden	0.018000	0.025500	0.033100	0.036164	0.040128
United Kingdom	0.057900	0.061000	0.064100	0.072232	0.080264
Switzerland	0.025946	0.028758	0.031575	0.035823	0.040106
Norway	0.019800	0.028050	0.036410	0.039780	0.044141
United States	0.072330	0.077450	0.116085	0.130850	0.123574
Canada	0.058810	0.062988	0.075613	0.078607	0.084678
Brazil	0.139791	0.149634	0.160640	0.185605	0.210848
Mexico	0.151893	0.170390	0.185800	0.222065	0.249432
Colombia	0.084907	0.107514	0.122931	0.145349	0.175136
Chile	0.078115	0.098160	0.113957	0.135465	0.171283
Argentina	0.074634	0.094827	0.110515	0.131250	0.159023
Australia	0.029530	0.030520	0.032260	0.037120	0.039200
Japan	0.058385	0.066449	0.104582	0.120306	0.119810
India	0.063542	0.069137	0.081946	0.088677	0.105390

China	0.026090	0.027411	0.031290	0.037050	0.039200
Malaysia	0.025517	0.027167	0.031222	0.037345	0.039383
Thailand	0.028294	0.034328	0.039700	0.043605	0.045298
Hong Kong	0.030363	0.039543	0.047625	0.053718	0.056751
South Korea	0.042124	0.049290	0.062762	0.066499	0.056589
Russia	0.109341	0.117054	0.142642	0.163121	0.172382
South Africa	0.017848	0.019703	0.026485	0.033674	0.035969
Nigeria	0.042221	0.049970	0.065981	0.077091	0.110861
Egypt	0.038180	0.045676	0.061699	0.072758	0.105691
Morocco	0.019090	0.022838	0.030850	0.036379	0.052846
Zambia	0.018249	0.027071	0.062289	0.076054	0.127481
Mozambique	0.017568	0.026045	0.062472	0.074848	0.124656
Global average	0.036115	0.041173	0.049502	0.056902	0.065876
Europe	0.021705	0.024261	0.026825	0.030383	0.034002
North America	0.065570	0.070219	0.095849	0.104728	0.104126
Central and South America	0.105868	0.124105	0.138768	0.163947	0.193144
Asia-Pacific	0.045910	0.051211	0.063781	0.071938	0.074889
Africa	0.025526	0.031884	0.051629	0.061801	0.092917

A7. DEMAND FOR CASH (CURRENCY/BROAD MONEY)					
	2014	2015	2016	2017	2018
Austria	0.090	0.091	0.091	0.090	0.088
Belgium	0.065	0.064	0.064	0.065	0.065
Bulgaria	0.150	0.154	0.160	0.165	0.167
Croatia	0.081	0.084	0.089	0.098	0.100
Cyprus	0.051	0.052	0.048	0.048	0.050
Czech Republic	0.130	0.130	0.134	0.130	0.127
Denmark	0.044	0.043	0.047	0.046	0.046
Estonia	0.178	0.172	0.164	0.161	0.156
Finland	0.104	0.104	0.105	0.103	0.101
France	0.090	0.093	0.092	0.089	0.090
Germany	0.086	0.084	0.081	0.080	0.079
Greece	0.135	0.176	0.184	0.181	0.183
Hungary	0.189	0.207	0.205	0.213	0.223
Ireland	0.075	0.081	0.079	0.079	0.076
Italy	0.108	0.111	0.111	0.110	0.113
Latvia	0.261	0.249	0.245	0.246	0.236
Lithuania	0.077	0.259	0.245	0.240	0.227
Luxemburg	0.008	0.009	0.009	0.009	0.009
Malta	0.057	0.055	0.053	0.051	0.052
Netherlands	0.060	0.065	0.066	0.069	0.072
Poland	0.123	0.130	0.138	0.139	0.141
Portugal	0.133	0.136	0.132	0.129	0.126
Romania	0.152	0.162	0.174	0.181	0.178
Slovakia	0.204	0.196	0.193	0.188	0.189
Slovenia	0.178	0.180	0.174	0.170	0.165
Spain	0.099	0.099	0.098	0.100	0.101
Sweden	0.031	0.026	0.020	0.017	0.017
United Kingdom	0.080	0.860	0.089	0.950	0.997
Switzerland	0.058	0.062	0.064	0.068	0.072
Norway	0.025	0.027	0.023	0.021	0.018
United States	0.078	0.081	0.082	0.085	0.086
Canada	0.058	0.061	0.062	0.058	0.057
Brazil	0.043	0.048	0.046	0.045	0.052
Mexico	0.177	0.183	0.187	0.183	0.188
Colombia	0.031	0.033	0.033	0.032	0.032
Chile	0.418	0.394	0.371	0.349	0.327
Argentina	0.044	0.044	0.044	0.046	0.046
Australia	0.036	0.037	0.036	0.039	0.038
Japan	0.072	0.074	0.074	0.075	0.076
India	0.158	0.162	0.074	0.146	0.162

China	0.049	0.045	0.044	0.042	0.041
Malaysia	0.045	0.049	0.053	0.055	0.052
Thailand	0.068	0.067	0.069	0.071	0.071
Hong Kong	0.042	0.042	0.042	0.042	0.043
South Korea	0.028	0.031	0.034	0.036	0.038
Russia	0.206	0.166	0.173	0.174	0.168
South Africa	0.030	0.030	0.030	0.031	0.033
Nigeria	0.064	0.065	0.067	0.065	0.059
Egypt	0.173	0.160	0.143	0.127	0.122
Morocco	0.046	0.046	0.048	0.051	0.055
Zambia	0.120	0.100	0.107	0.105	0.103
Mozambique	0.103	0.090	0.099	0.094	0.088
Global average	0.101	0.120	0.102	0.119	0.119
Europe	0.104	0.139	0.113	0.141	0.142
North America	0.068	0.071	0.072	0.071	0.071
Central and South America	0.167	0.140	0.136	0.131	0.129
Asia-Pacific	0.078	0.075	0.067	0.076	0.077
Africa	0.089	0.085	0.082	0.079	0.077

A8. TRANSFERABLE DEPOSITS/TOTAL DEPOSITS (%)

	2014	2015	2016	2017	2018
Austria	0.564	0.611	0.654	0.696	0.725
Belgium	0.323	0.331	0.368	0.379	0.381
Bulgaria	0.362	0.393	0.420	0.469	0.489
Croatia	0.367	0.406	0.490	0.575	0.663
Cyprus	0.306	0.340	0.375	0.402	0.464
Czech Republic	0.818	0.842	0.878	0.877	0.865
Denmark	0.831	0.874	0.886	0.892	0.910
Estonia	0.737	0.793	0.806	0.838	0.832
Finland	0.730	0.761	0.793	0.811	0.864
France	0.369	0.402	0.420	0.448	0.459
Germany	0.646	0.675	0.692	0.708	0.726
Greece	0.415	0.610	0.633	0.645	0.640
Hungary	0.476	0.583	0.709	0.804	0.818
Ireland	0.433	0.488	0.496	0.521	0.536
Italy	0.651	0.679	0.719	0.742	0.760
Latvia	0.786	0.822	0.825	0.845	0.845
Lithuania	0.709	0.746	0.790	0.810	0.815
Luxemburg	0.577	0.589	0.609	0.631	0.635
Malta	0.640	0.734	0.749	0.782	0.794
Netherlands	0.491	0.480	0.435	0.437	0.435
Poland	0.515	0.541	0.589	0.636	0.655
Portugal	0.377	0.437	0.464	0.491	0.527
Romania	0.355	0.430	0.483	0.514	0.534
Slovakia	0.633	0.667	0.706	0.730	0.757
Slovenia	0.518	0.616	0.678	0.729	0.761
Spain	0.582	0.637	0.698	0.784	0.825
Sweden	0.730	0.760	0.808	0.811	0.805
United Kingdom	0.468	0.541	0.617	0.630	0.656
Switzerland	0.402	0.393	0.424	0.440	0.463
Norway	0.465	0.686	0.911	0.907	0.930
United States	0.124	0.123	0.123	0.134	0.126
Canada	0.196	0.211	0.235	0.276	0.309
Brazil	0.058	0.047	0.043	0.042	0.041
Mexico	0.382	0.383	0.378	0.373	0.369
Colombia	0.253	0.233	0.225	0.220	0.220
Chile	0.254	0.213	0.228	0.199	0.190
Argentina	0.333	0.336	0.326	0.352	0.347
Australia	0.399	0.424	0.427	0.440	0.440
Japan	0.468	0.476	0.508	0.530	0.550
India	0.092	0.093	0.108	0.110	0.106

China	0.361	0.380	0.409	0.422	0.399
Malaysia	0.216	0.220	0.223	0.230	0.215
Thailand	0.031	0.033	0.031	0.034	0.032
Hong Kong	0.148	0.146	0.148	0.146	0.141
South Korea	0.274	0.307	0.321	0.326	0.309
Russia	0.230	0.212	0.232	0.241	0.237
South Africa	0.258	0.262	0.271	0.271	0.263
Nigeria	0.329	0.324	0.369	0.358	0.338
Egypt	0.208	0.216	0.201	0.200	0.204
Morocco	0.542	0.548	0.563	0.581	0.592
Zambia	0.559	0.564	0.616	0.586	0.617
Mozambique	0.651	0.621	0.626	0.603	0.617
Global average	0.435	0.466	0.495	0.513	0.524
Europe	0.543	0.595	0.638	0.666	0.686
North America	0.160	0.167	0.179	0.205	0.218
Central and South America	0.256	0.242	0.240	0.237	0.233
Asia-Pacific	0.247	0.254	0.268	0.275	0.270
Africa	0.425	0.422	0.441	0.433	0.439

A9. SHADOW ECONOMY/GDP (%)					
	2014	2015	2016	2017	2018
Austria	8.2	8.2	9.0	8.3	8.6
Belgium	18.0	17.3	17.4	17.0	17.3
Bulgaria	22.8	22.3	24.1	23.1	22.1
Croatia	25.4	25.2	25.3	24.9	24.9
Cyprus	31.6	31.9	32.1	32.2	32.7
Czech Republic	11.2	11.1	12.8	12.2	11.9
Denmark	14.3	14.9	15.2	14.9	15.2
Estonia	18.3	18.6	18.4	18.2	17.8
Finland	11.4	11.6	11.8	11.9	12.4
France	12.8	12.4	12.2	12.2	11.7
Germany	8.3	8.0	7.8	7.9	7.8
Greece	26.4	27.6	27.8	28.2	29.3
Hungary	22.4	21.7	21.2	20.7	20.4
Ireland	11.5	11.2	11.0	10.6	10.7
Italy	24.9	24.9	25.1	25.4	25.1
Latvia	16.4	17.0	16.2	16.1	16.4
Lithuania	17.6	18.3	18.6	18.1	18.5
Luxemburg	10.4	10.6	10.4	10.2	10.9
Malta	28.1	28.4	28.2	28.9	29.1
Netherlands	8.3	8.6	8.2	7.9	7.5
Poland	18.1	18.0	17.4	17.1	16.7
Portugal	21.4	20.7	20.4	20.5	20.1
Romania	23.1	23.3	24.2	24.6	23.2
Slovakia	12.0	11.8	12.0	11.3	11.1
Slovenia	24.3	23.6	22.8	23.0	22.2
Spain	21.3	21.1	21.2	20.9	20.1
Sweden	11.2	11.3	11.3	11.9	12.3
United Kingdom	9.5	9.3	9.3	8.9	8.5
Switzerland	6.2	6.4	6.5	6.2	6.9
Norway	15.1	15.3	15.0	15.8	16.2
United States	8.5	8.1	8.3	8.1	8.0
Canada	10.1	9.8	9.4	9.6	9.0
Brazil	33.1	34.5	35.9	33.2	32.1
Mexico	30.4	30.6	31.2	31.8	31.9
Colombia	26.4	27.0	26.2	26.0	25.7
Chile	15.0	14.3	13.9	13.5	12.4
Argentina	25.0	26.4	28.5	30.3	31.7
Australia	8.9	8.4	8.4	8.2	8.2
Japan	9.3	9.1	8.9	8.4	8.2

India	20.4	21.2	20.1	20.0	19.9
China	12.0	11.2	11.1	11.2	11.0
Malaysia	29.1	28.7	28.4	27.9	27.3
Thailand	47.3	48.6	47.9	46.3	46.0
Hong Kong	12.2	12.4	12.0	11.8	11.9
South Korea	21.4	21.0	20.8	20.5	19.9
Russia	32.9	33.2	33.1	34.3	35.2
South Africa	23.6	23.3	24.1	23.3	22.9
Nigeria	50.5	50.2	51.3	52.0	51.8
Egypt	35.7	36.1	36.6	37.1	37.5
Morocco	30.2	30.1	29.8	29.9	29.7
Zambia	36.2	37.9	35.1	34.4	34.0
Mozambique	33.4	33.2	34.1	33.2	31.9
Global average	20.4	20.5	20.5	20.4	20.3
Europe	17.0	17.0	17.1	17.0	16.9
North America	9.3	8.9	8.8	8.9	8.5
Central and South America	26.0	26.6	27.1	27.0	26.7
Asia-Pacific	21.5	21.5	21.2	21.0	20.8
Africa	34.9	35.1	35.1	35.0	34.7

A10. ILLEGAL ECONOMY CONDUCTED WITH CASH/GDP (%)					
	2014	2015	2016	2017	2018
Austria	0.9	0.9	0.9	0.9	0.9
Belgium	3.3	3.2	3.0	3.0	2.8
Bulgaria	4.1	4.1	4.1	4.0	4.1
Croatia	4.2	4.2	4.1	4.0	3.9
Cyprus	7.0	7.3	7.3	7.1	6.8
Czech Republic	2.1	2.2	2.0	1.9	2.1
Denmark	2.1	2.2	2.4	2.5	2.7
Estonia	2.7	2.5	2.5	2.6	2.6
Finland	1.9	1.9	2.1	2.0	2.0
France	2.3	2.2	2.0	1.9	1.9
Germany	1.1	1.0	0.9	0.9	0.9
Greece	7.9	7.9	7.5	7.6	6.9
Hungary	5.0	4.5	4.3	4.1	4.0
Ireland	2.7	2.5	2.3	2.5	2.2
Italy	7.6	7.6	7.1	6.9	6.3
Latvia	3.2	3.0	2.9	3.0	2.7
Lithuania	3.8	3.9	3.6	3.5	3.2
Luxemburg	1.9	1.6	1.8	1.7	1.7
Malta	7.2	7.3	7.0	6.6	6.6
Netherlands	1.2	1.1	1.1	1.0	1.1
Poland	3.0	2.7	2.4	2.2	2.1
Portugal	5.2	5.1	4.9	4.9	4.6
Romania	7.9	7.9	7.4	7.2	7.0
Slovakia	2.1	2.0	2.1	1.9	1.7
Slovenia	4.6	4.6	4.2	4.0	4.1
Spain	6.1	5.4	5.1	5.0	4.7
Sweden	3.3	3.2	3.4	3.4	3.4
United Kingdom	2.2	2.0	2.0	1.8	1.7
Switzerland	0.8	0.7	0.6	0.6	0.6
Norway	3.9	3.6	3.9	3.9	4.0
United States	2.5	2.3	2.2	2.2	2.1
Canada	2.2	2.1	2.0	2.2	1.9
Brazil	9.9	9.6	9.1	8.9	8.8
Mexico	10.6	10.6	10.2	10.0	10.2
Colombia	8.9	9.0	8.7	8.3	8.3
Chile	3.8	3.6	3.1	2.9	2.7
Argentina	7.3	7.4	7.1	7.0	6.9

Australia	1.5	1.4	1.4	1.2	1.0
Japan	2.4	2.4	2.3	2.2	2.1
India	4.4	4.2	4.0	4.0	3.7
China	2.1	2.0	2.0	2.0	2.0
Malaysia	10.0	9.9	9.6	9.5	9.6
Thailand	12.9	13.1	13.2	13.6	13.6
Hong Kong	2.0	2.2	1.8	1.9	1.6
South Korea	5.9	5.8	5.6	5.3	5.3
Russia	11.9	12.0	11.7	12.3	12.3
South Africa	6.4	6.4	6.2	6.1	6.0
Nigeria	14.5	14.7	15.0	14.3	14.0
Egypt	9.1	9.2	9.3	9.6	9.5
Morocco	9.3	9.3	9.0	8.9	8.9
Zambia	11.0	10.6	10.8	10.6	10.2
Mozambique	9.3	9.1	9.0	9.2	9.2
Global average	5.2	5.1	5.0	4.9	4.8
Europe	3.7	3.6	3.5	3.4	3.3
North America	2.4	2.2	2.1	2.2	2.0
Central and South America	8.1	8.0	7.6	7.4	7.4
Asia-Pacific	5.9	5.9	5.7	5.8	5.7
Africa	9.9	9.9	9.9	9.8	9.6

A11. SHADOW ECONOMY (LEGAL ORIGIN BUT TAX EVADED)/GDP (%)

	2014	2015	2016	2017	2018
Austria	7.3	7.3	8.1	7.4	7.7
Belgium	14.8	14.1	14.4	14.1	14.5
Bulgaria	18.8	18.2	20.0	19.1	18.1
Croatia	21.2	21.0	21.2	20.8	21.0
Cyprus	24.5	24.6	24.8	25.1	25.9
Czech Republic	9.1	8.9	10.7	10.3	9.8
Denmark	12.2	12.7	12.9	12.4	12.5
Estonia	15.6	16.1	15.9	15.7	15.1
Finland	9.4	9.7	9.7	10.0	10.4
France	10.5	10.2	10.2	10.3	9.8
Germany	7.1	7.0	6.9	7.0	6.9
Greece	18.5	19.7	20.3	20.5	22.4
Hungary	17.4	17.2	16.9	16.6	16.4
Ireland	8.9	8.7	8.7	8.1	8.5
Italy	17.3	17.3	18.0	18.4	18.9
Latvia	13.2	14.0	13.3	13.1	13.7
Lithuania	13.8	14.4	15.0	14.6	15.3
Luxemburg	8.5	9.0	8.6	8.5	9.2
Malta	20.9	21.1	21.2	22.4	22.5
Netherlands	7.1	7.4	7.2	6.9	6.5
Poland	15.1	15.3	15.0	14.9	14.6
Portugal	16.2	15.6	15.5	15.6	15.5
Romania	15.2	15.4	16.8	17.4	16.1
Slovakia	9.9	9.8	9.9	9.4	9.4
Slovenia	19.6	19.0	18.6	19.0	18.1
Spain	15.2	15.7	16.0	16.0	15.4
Sweden	7.9	8.1	8.0	8.5	8.9
United Kingdom	7.4	7.2	7.4	7.2	6.8
Switzerland	5.5	5.7	5.9	5.5	6.4
Norway	11.2	11.7	11.1	11.9	12.2
United States	6.0	5.8	6.1	5.9	5.9
Canada	7.8	7.7	7.3	7.4	7.1
Brazil	23.2	24.8	26.8	24.4	23.3
Mexico	19.8	20.0	21.0	21.7	21.8
Colombia	17.5	18.0	17.5	17.7	17.4
Chile	11.2	10.7	10.8	10.6	9.6
Argentina	17.7	19.0	21.4	23.2	24.7
Australia	7.4	7.0	7.0	7.0	7.2
Japan	6.9	6.6	6.6	6.1	6.1

India	16.0	17.0	16.1	16.1	16.1
China	10.0	9.2	9.1	9.3	9.0
Malaysia	19.1	18.9	18.8	18.4	17.8
Thailand	34.3	35.5	34.7	32.7	32.4
Hong Kong	10.1	10.2	10.2	10.0	10.3
South Korea	15.5	15.2	15.2	15.2	14.6
Russia	21.0	21.3	21.4	22.0	22.9
South Africa	17.2	16.9	17.8	17.2	16.9
Nigeria	36.0	35.5	36.3	37.8	37.8
Egypt	26.6	26.9	27.3	27.4	28.0
Morocco	20.9	20.7	20.8	21.1	20.8
Zambia	25.2	27.2	24.2	23.8	23.9
Mozambique	24.0	24.1	25.0	24.0	22.7
Global average	15.2	15.4	15.6	15.5	15.5
Europe	13.3	13.4	13.6	13.6	13.6
North America	6.9	6.8	6.7	6.7	6.5
Central and South America	17.9	18.5	19.5	19.5	19.4
Asia-Pacific	15.6	15.6	15.5	15.2	15.2
Africa	25.0	25.2	25.2	25.2	25.0