The Hidden Costs of Card Payments

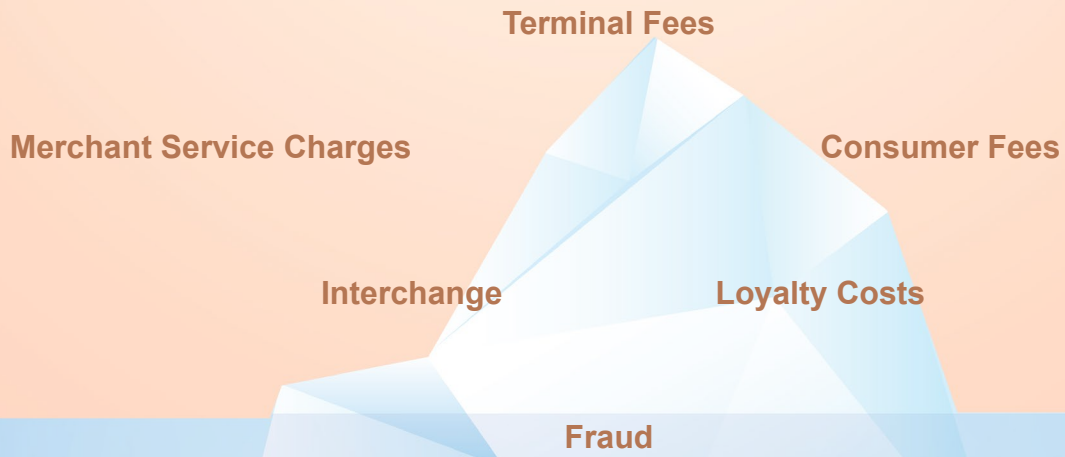
by
Diederik Bruggink
and Guillaume Lepecq

December 2016

Cash Essentials
www.cashessentials.org

The Hidden Cost of Cards

Current research has taken only the direct costs of card payments into account. A plethora of other less visible cost items for card transactions can be identified as well. If these hidden costs would be quantified, it would add significantly to the cost of card payments.



Card fraud totalled $21.84 in 2015, a 20.6% annual increase.

Outages and Breakdowns

In 2013, the Belgian card scheme broke down a few hours before Christmas.

Failed Transactions

68.81% of online shopping carts are abandoned before checkout. Payment is an important factor behind this

Protection against Fraud

Compliance with industry Standards to reduce fraud can cost upwards of $500,000 per year for large merchants.

Regulatory Compliance

Mauritius has more government officials working on Anti-Money Laundering implementation than the country has opticians.

Data Breaches

Over 4.8 billion personal records have been exposed since 2013.

Other costs

Bitcoin consumes as much energy as all of Ireland.

The Hidden Costs of Card Payments

Diederik Bruggink
Bruggink Consultancy

Guillaume Lepecq
AGIS Consulting

Introduction

Payments are a big business: according to the Boston Consulting Group[1], banks handle non-cash payments equal to more than five times global GDP and earn related revenues of USD 1.1 trillion. The calculated payments revenues include direct and indirect revenues generated by electronic payment services (excluding interbank transfers).

BNP and Capgemini[2] indicate in the World Payments Report 2016, that cards have been the fastest growing payments instrument since 2010. Debit cards accounted for the highest share (45.7%) of global electronic transactions and were also the fastest growing (12.8%) payment instrument in 2014. In spite of the hype and media attention, mobile payments only play a marginal role in terms of volume as can be seen from Figure 1 (most mobile payments are in fact contactless payments but not all contactless payments are mobile payments).

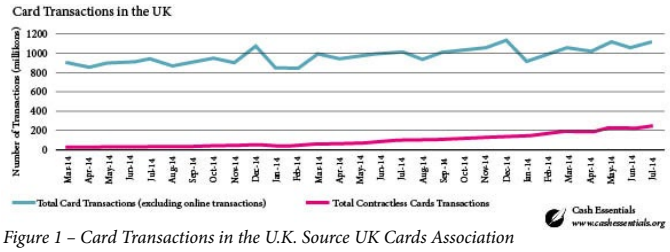


Figure 1 – Card Transactions in the U.K. Source UK Cards Association

Most of the research focusing on the cost of payments looks at the real, visible and tangible costs and compares them to the cost of cash. There are, however, more costs associated with payments than those direct costs.

The purpose of this paper is to look at the 'hidden' costs of card payments, in order to be able to make a fair comparison to the cost of cash. Where possible these hidden costs are quantified, but in some cases the indication of these costs will be more qualitative.

A brief recap of the visible cost of card payments will be provided in the first section. It is followed by a deep dive in the hidden costs, in Section 2. Section 3 consists in comparison with the cost of cash. It is followed by a conclusion.

1 https://www.bcgperspectives.com/content/articles/financial-institutions-technology-digital-global-payments-2016-competing-open-seas

2 World Payments Report 2016, BNP and Capegemini, https://www.worldpaymentsreport.com

1. The Visible Costs of Card Payments

Breakdown of Card Acceptance Costs for merchants

Retailers face a variety of visible costs, when they decide to accept cards. This is inherent to most business models under which cards operate. The majority of the card transactions take place under a model, where four parties can be identified: the cardholder, the cardholder bank (issuer or issuing bank), the retailer and the retailer bank (acquirer or acquiring bank). This model is referred to as the four-party model, and in this model only the banks have a relationship with the card schemes. Well-known schemes like MasterCard UnionPay or Visa operate under this model.

Merchants are expected to pay for their terminals (via a buy or lease construction) and for the maintenance of their terminals. They are expected to pay for the connectivity of the terminal to the network and their acquiring bank will charge a fee per transaction in the form of a Merchant Service Charge (MSC). In addition, if retailers wish to participate in a card related loyalty scheme, this will also come with a cost.

Whilst the costs related to terminals, their maintenance and their connectivity is quite transparent, understanding the pricing from the acquiring banks for card acceptance is far more complex. The latter is mainly driven by the fact that the acquirers themselves face a variety of costs that need to be factored into their pricing towards retailers. The main cost drivers that bank acquirers are facing are interchange fees (fees that are paid to issuers), card scheme fees (brand fees that are paid to the card schemes), processing fees (fees for clearing and settlement) and their own costs and mark-up. Figure 2 outlines the various fees that are being paid in the four-party model.

Interchange fees are ultimately paid to the banks that issues the card, and are usually a percentage of the transaction. Whilst in some jurisdictions, such as the European Union these are regulated, interchange fees can be a significant cost of the final transaction price. Card scheme fees are paid to the card schemes for using the brand on the card and for the processing (clearing and settlement) of the transaction. In some jurisdictions, the actual processing could be performed by an independent switch instead of by the card schemes; in that case, these charges would not be paid to the card schemes, but to the switch.

Apart from these external costs, acquiring banks incur internal costs as well. Whether they have outsourced part of their processing to an external vendor or not, these costs need to be factored in as well. Finally, an acquirer will factor in a mark-up in order to generate profit.

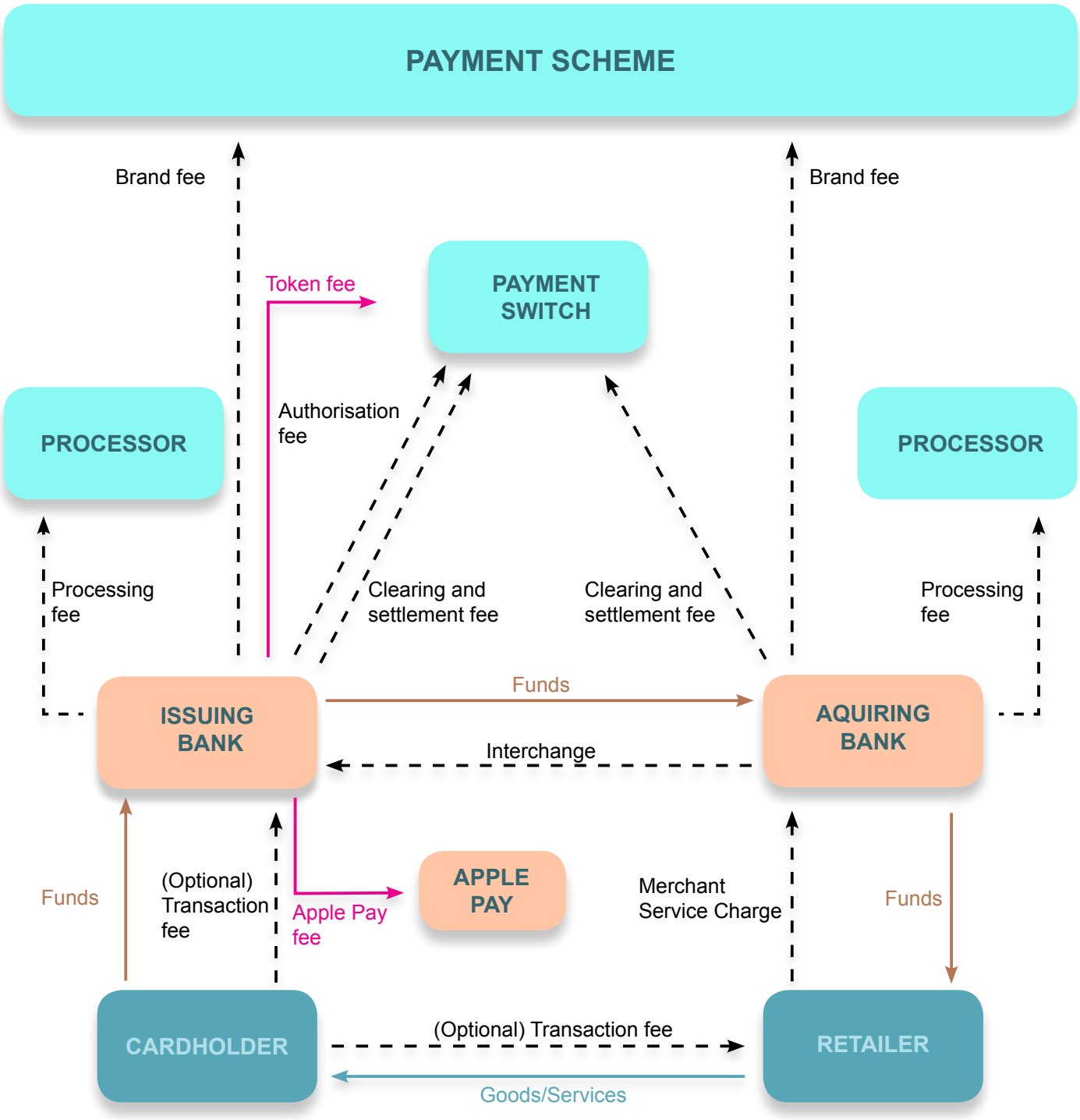
Until recently, it was common practice for acquirers to charge a single, blended fee to their retailers, which meant that retailers would not be aware of the various cost drivers. Also, interchange levels were one of the best-kept secrets in the banking industry, and it was not until regulators started to interfere, that transparency started to increase. As the EU Competition Commissioner said in 2009 in a press release: "*I am satisfied that these undertakings will not only improve the efficiency and transparency of the MasterCard payment card scheme but also provide a fair share of the benefits to consumers and retailers. The new methodology for calculating the MIF will help to bring clarity for banks and retailers and also lead to a substantial reduction in comparison to MasterCard's previous MIF. We will be monitoring implementation closely in the coming months*[3]". The Chair of the US Federal Reserve System stated in 2011: "*The debit card success story has been marred by the level of discord between merchants and issuers on the interchange fee issue, which has played out in the courts, in the Congress, and more recently here at the Board. The continued vitality of the debit card system requires balancing of the legitimate needs of depository institutions that issue debit cards, merchants that accept them, networks that process them, and, very importantly, the consumers who are the customers of both the banks and the merchants*"[4].

However, due to pressure from the retail industry and from regulators, in some jurisdictions interchange fees are now published and in some areas even regulated (see page 8). In the European Union, acquirers are now mandated (unless agreed differently with their retailers) to include in their agreements, individually specified information on the composition of the merchant service charges, interchange fees and scheme fees applicable with respect to each category and brand of payment cards, aiming to increase transparency on card transaction pricing.

3 http://europa.eu/rapid/press-release_IP-09-515_en.htm?locale=en

4 http://www.federalreserve.gov/newsevents/press/bcreg/yellen20110629a1.htm

Figure 2 - Actors and Flows in the Four Party Card Model.



Source: Diederick Bruggink

Cash Essentials
www.cashessentials.org

Loyalty

Loyalty programs can come in different shapes and sizes, with various costs associated with them. Some are tied to the payment card itself and deliver benefits to the customer every time the card is used, for example in the form of airline miles, cash-backs or extended guarantee. These benefits are funded by the bank or the related loyalty partner, for instance the airline. This means retailers are not bearing any costs for these, although in most cases, these programmes are funded partially by the interchange fees mentioned above. These card programmes stimulate card usage and are not necessarily creating loyalty to a specific retailer.

Alternatively, merchants can choose to participate in a so-called merchant-funded loyalty programme. In this case, retailers provide rewards and incentives and the programmes can be sponsored by issuing banks. Consumers can earn loyalty points or rewards by using a bank card at a participating retailer. In such a set-up, the retailer agrees to fund the points, with cash-back or discounts, in exchange for marketing exposure. In such a loyalty scheme, retailers face additional costs in return of better exposure.

Costs for consumers

Cardholders also face a variety of costs when using their cards. Some of these costs may be clear to them, like annual card fees, ATM fees, per transaction charges and surcharges imposed on them by retailers; other costs, like a foreign-exchange mark-up when making transactions in another currency may be less transparent. Also, the part of the card-related fees that banks charge and that are used to finance insurances that are tied to some cards is not always clear.

As issuing banks are receiving less interchange due to various regulations, they might seek to increase their card pricing towards consumers. Research from First Annapolis[5], covering activity from January through July 2016, confirms their initial hypothesis that as a result of the interchange regulation, European issuers continue to rationalize their product set, reduce rewards value, and rely more on fees to drive product revenues: annual fees have continued to increase since January. In Spain, Portugal, France, and Italy, almost half of the top five to six issuers have raised their annual card fees. In France, some banks have increased annual fees on cards by 2% on average. In Spain, the average increase was as high as 26% for cards that saw an upwards price adjustment. In Germany, where the reduction in interchange was significant and where the cap hit hard on credit cards interchange, several large, well known issuers are now charging on average 20% more for some of their card offerings than they did in the beginning of 2016. Additionally, one of the largest banks in the Netherlands has increased fees on some of its credit cards by 60%.

First Annapolis also concluded that Issuers have also continued increasing credit card Annual Percentage Rates[6] (APRs) since January to compensate for the revenue lost from interchange regulation. Markets where most issuers have increased their APRs include Portugal, Poland, and Italy, where rates have increased by 30 bps, 100 bps, and 131 bps, respectively. European issuers have also continued raising fees on other products and services. In France, a bank has increased the fee when consumers choose their own PIN. In the Czech Republic, a bank has added additional fees for transactions made at gambling and adult-services merchants, and also increased ATM cash withdrawal fees. Some banks in Belgium, Portugal and Denmark have also increased ATM cash withdrawal fees on some cards.

2. Hidden Costs of Card Payments

Apart from the more visible - but not necessarily transparent - costs mentioned in the previous section, there are also additional costs involved in payments that are less visible. Although some of these costs might be 'absorbed' by the system, most systems will externalise these costs in the form of higher charges to the users of the card payment system. Consumers might face higher fees for their cards, but may also face higher prices for the goods they want to purchase as retailers will factor in the total costs they are paying for card payments. Part of the hidden costs are also social costs – additional law enforcement might be required to fight fraud or to combat cybercrime. Some of the hidden costs of card payments will be covered in more detail in this section.

5 http://www.firstannapolis.com/articles/six-months-after-in-terchange-regulation-in-the-eu-how-have-card-products-changed

6 APR is an annual percentage rate of interest a credit card holder will be charged on all or a portion of the balance if the full amount isn't paid on or before the due date.

Interchange Regulation Globally[1]

Australia and New Zealand

In 2003, the Reserve Bank of Australia (RBA) is the first regulator to have addressed market failures in the payment card sector by lowering the level of interchange fees and by changing network rules in order to increase competition. After having received the power to regulate payment systems in 1998, and having carried out some research, the RBA concluded that: "Co-operative behaviour [...] is anti-competitive and, where it is allowed, it typically requires some form of dispensation by competition authorities on the basis that there are offsetting benefits to the public". In 2003, Visa and MasterCard's MIF were lowered from approximately 0.95 to 0.55%. Apart from capping interchange fees, the RBA modified network rules, prohibiting "no surcharge rules" and "honour all cards rules". Moreover, the RBA encouraged increased transparency in retail payment systems.

In 2006, the New Zealand Commerce Commission issued proceedings against Visa and MasterCard, alleging that interchange fees constitute price fixing and result in a substantial lessening of competition. Shortly before the court case was due to start in Autumn 2009, the suit was settled out of court; the "no surcharge rule" was prohibited, allowing retailers to pass on the cost of MasterCard and Visa transactions to the customer, and card issuers were allowed to set their own interchange fees, within a maximum limit set by Visa or MasterCard. All issuers of MasterCard cards in New Zealand announced they would be charging the maximum rate. The Commission released a report in 2013 reviewing the outcome of the settlement, showing that many merchants were paying higher fees for accepting credit cards than before the settlement.

---

1 European Credit Research Institute (ECRI), 'Multilateral Interchange Fees: Competition and Regulation in light of Recent Legislative Developments', January 2014, ISBN 978-94-6138-375-4 (Authors Maria Chiara Malaguti and Alessandra Guerrieri).

United States

Senate hearings in the United States have focused on the secrecy surrounding interchange fee schedules and card operating rules. In 2006 Visa and MasterCard both released some fee schedules and summary reports of their card rules, though pressure continues for them to release the full documents. In January 2007, Senate Banking committee chairman Chris Dodd cited interchange fees at a hearing on credit card industry practices and again in March the fees were criticized by Sen. Norm Coleman. In January 2007, Microsoft chairman Bill Gates cited high interchange fees as a significant reason Microsoft believes it can't be competitive in online micropayments.

On October 1, 2010, the Durbin Amendment came into effect. The Durbin Amendment imposes that interchange fees for any electronic debit transaction be "reasonable and proportional to the cost incurred by the issuer with respect to the transaction", and asks the Fed to prescribe regulations to establish standards for

determining whether fees are "reasonable" and "proportional". On 20 July 2011, the Board set the maximum level of interchange fees for debit card transactions at 21 cents per transaction and 5 basis points multiplied by the value of the transaction. At the same time, issuers implementing certain fraud-prevention measures were allowed to increase their interchange fees by as much as one cent. This cap took effect from 1 October 2011.

European Union

In January 2007, the European Commission issued the results of a two-year inquiry into the retail banking sector. The report focuses on payment cards and interchange fees. Upon publishing the report, the EU Competition Commissioner said the "present level of interchange fees in many of the schemes we have examined does not seem justified." The report called for further study of the issue.

In 2009 MasterCard undertook to lower its cross-border consumer MIF to 0.20% for debit and 0.30% for credit cards, and made many changes to the business rules. Similar commitments were offered by Visa Europe in 2010 for consumer debit, and in 2013 for consumer credit cards. Finally, the French Competition Authority made binding commitments offered in 2010 by the Groupement des Cartes Bancaires to set its MIF for domestic transactions at equivalent levels. In March 2015, the European Parliament voted to cap interchange fees to 0.3% for credit cards and to 0.2% for debit cards, which was subsequently enacted under Regulation (EU) 2015/751 with effect from 8 June 2015. The caps apply only to personal cards where there is an intermediary, not to cards issued to businesses or to cards issued by American Express.

Card Fraud

Card fraud totalled $21.84 billion in 2015, a 20.6% annual increase.

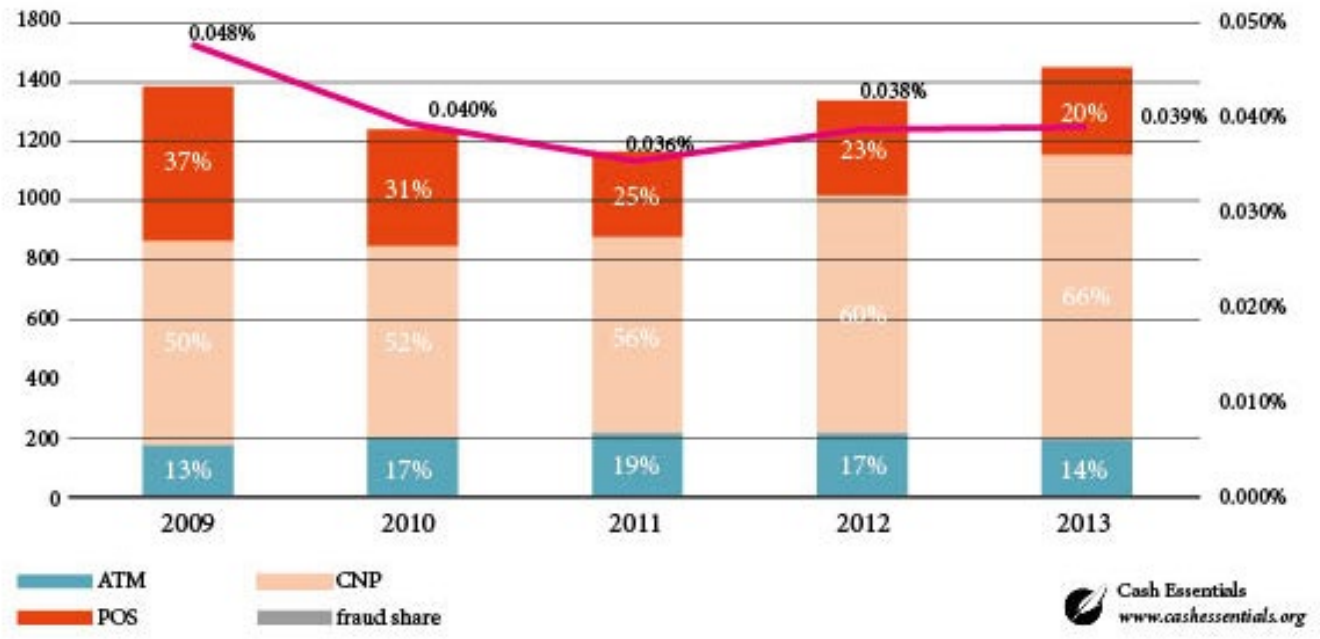
The Nilson Report[7] a leading publication covering payment systems worldwide, published in October 2016 that gross fraud losses to criminals incurred by issuers, merchants and acquirers totalled $21.84 billion in 2015, which is a whopping increase of 20.6% over the 2014 figures. Card issuers lost 72% of this fraud, whilst merchants and acquirers accounted for the other 28%. Those losses do not include related costs issuers, merchants, and acquirers incur (these will be covered later in this section).

Most of the card related fraud is happening in the so-called card-not-present (CNP) environment, i.e. in transactions where the card actually cannot be used physically, such as in e-commerce and m-commerce transactions. According to the European Central Bank (ECB)[8], in Europe, in 2013, 66% of the value of fraud resulted from CNP payments, i.e. payments via the internet, post or telephone, 20% from transactions at point-of-sale (POS) terminals and 14% from transactions at automated teller machines (ATMs). Historical data is presented in Figure 3, in which the card fraud share is presented as the share of the total value of card transactions.

The ECB identified that most of the countries with mature card markets (defined as countries with high volumes and values of card transactions per inhabitant) experienced high rates of fraud, as can be seen in Figure 4. CNP fraud was typically the most common type of fraud experienced on cards issued in these markets. By contrast, countries with limited card usage experience relatively low levels of fraud. Owing to limited use, the potential financial gains are lower and, since EMV migration is almost complete, it is much easier to target non-EMV countries outside SEPA.

Over 1 million incidents of financial fraud occurred in the first six months of 2016 in the UK alone, according to official figures released by Financial Fraud Action UK (FFA UK)[9]. This represents a 53% increase, compared to the same period last year. This means an incident happened in the UK every 15 seconds between January and June 2016. The figures are released as FFA UK and all major banks and key financial services providers across the UK come together for the first time to launch a national campaign to combat financial fraud. Financial fraud losses across payment cards, remote banking and cheques totalled £755.0 million in 2015, an increase of 26% compared to 2014. 75% of these losses are attributed to cards, as can be seen in Figure 5.

Figure 3 - Evolution of the total value of card fraud using cards issued within SEPA in 2013. Source ECB. (EUR millions: value of fraud as share of value of transactions)



7 http://www.prweb.com/releases/creditcardfraud/2015/prweb13791784.htm

8 European Central Bank, 'Fourth Report on Card Fraud', July 2015.

9 https://www.financialfraudaction.org.uk

Figure 4 - Card fraud levels in basis points and card transaction value per inhabitant per European country in 2013. Source Diederik Bruggink based on ECB data over 2013.

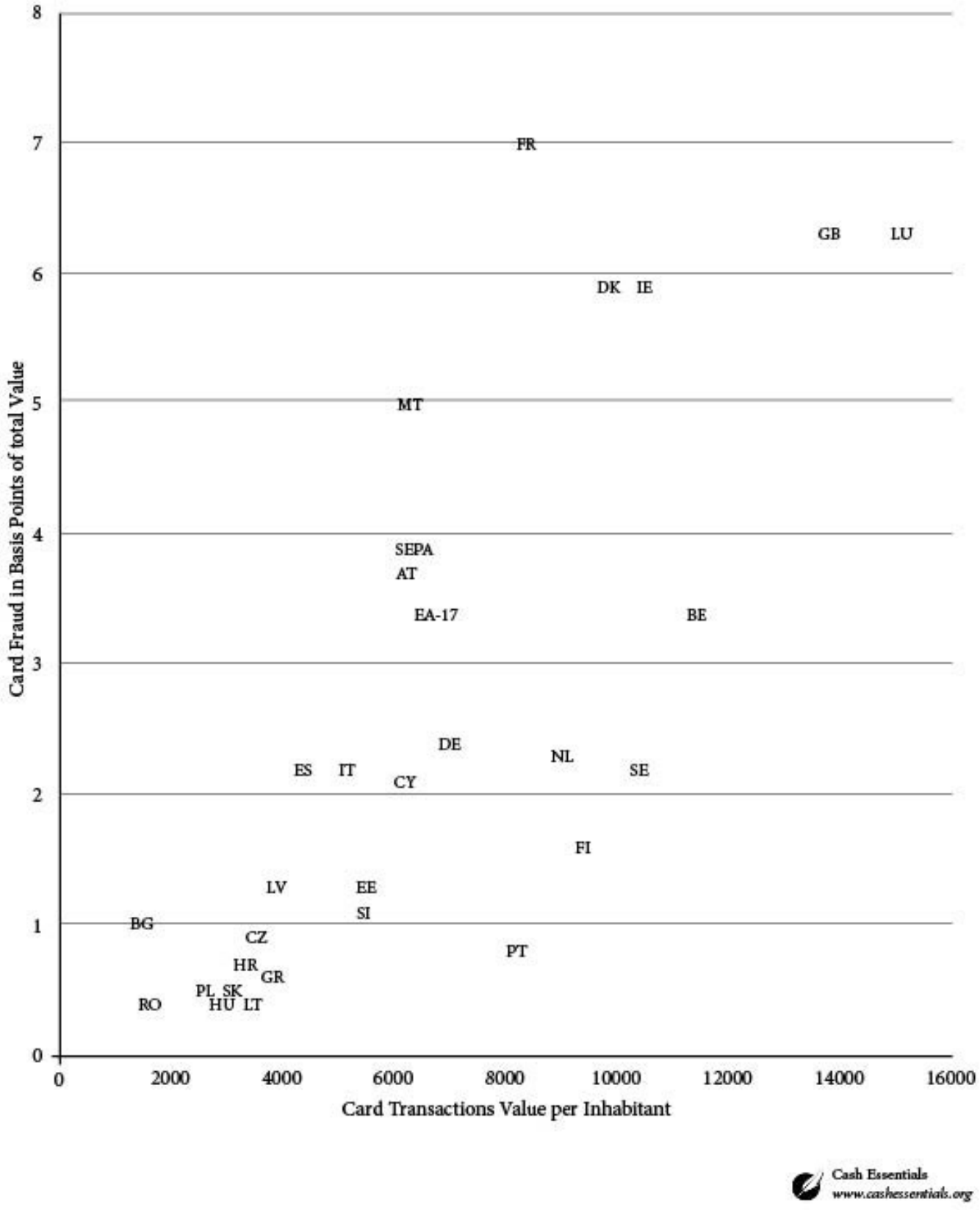
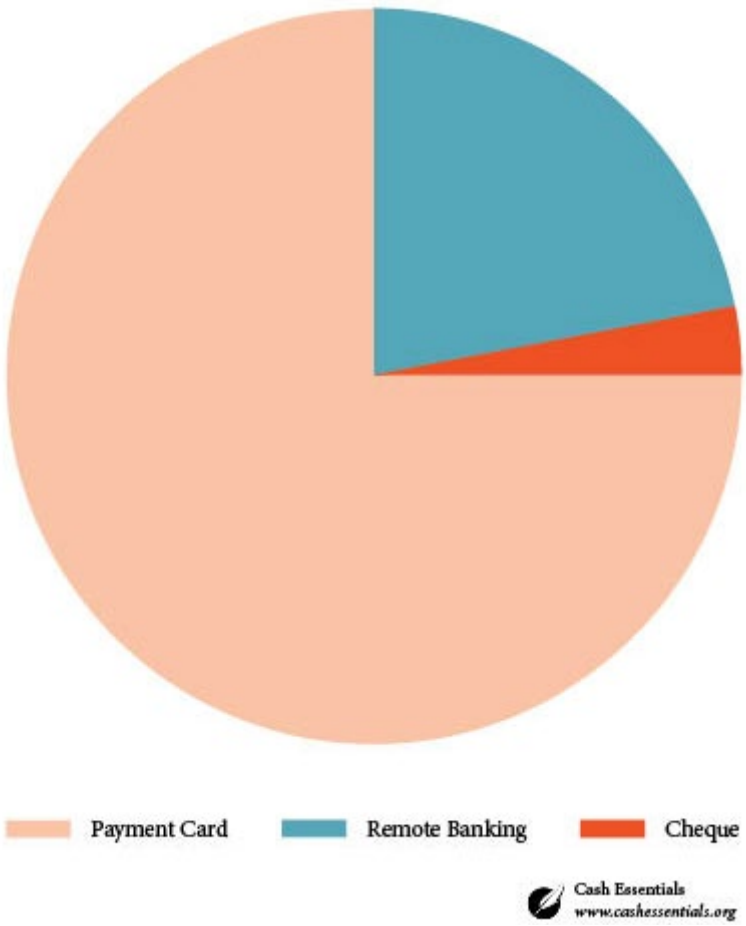


Figure 5 - 2015 Financial Fraud Losses by type. Source FFA UK.



LexisNexis, in their 2016 True Cost of Fraud Study[10], have analysed fraud that the merchant community is facing in the broadest sense of the word, so their analysis is not limited to card transactions only. Their research covers consumer-facing retail fraud methods and does not include information on insider fraud or employee theft. They have introduced the concept of the LexisNexis Fraud Multiplier, which is the total amount of costs related to fees, interest, merchandise replacement and redistribution per dollar of fraud for which the merchant is held liable. On average, US merchants reported an 8% increase over the previous year in the cost per dollar of fraud losses, from $2.23 to $2.40, as can be derived from the Study. This means that for every dollar of losses, merchants are losing $2.40 based on chargebacks, fees and merchandise replacement.

LexisNexis found that US merchants continue to experience increased fraud losses in 2016, particularly among larger merchants with remote channel transactions. Large eCommerce and mCommerce merchants are challenged on various fronts, including an increased volume of successful fraud attempts, a rise in fraud cost/dollar losses and a bigger bite of fraud costs as a percentage of annual revenues. At the same time, these large remote merchants are investing in resources to combat these issues, ranging from adopting multiple fraud mitigation solutions, to the use of automated fraud flagging systems. That said, there is frustration with the cost of managing fraud, while still battling the expense of manual reviews and challenges of false positives. In fact, large remote merchants who use an automated flagging system and multiple fraud mitigation solutions still send a sizeable portion of flagged transactions for manual review, suggesting that they don't fully trust their solutions to delineate between legitimate and fraudulent customers.

Protection against fraud

Compliance with industry standards to reduce fraud can cost upwards of $500,000 per year for large merchants.

Considering the growing size of the fraud problem, stakeholders in the payments value chain have been reinforcing measures to protect themselves.

In order to prevent payment data being stolen, the

10 LexisNexis 2016 True Cost of Fraud Study, May 2016.

industry came up with a proprietary information security standard for all organizations that store, process or transmit branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. Compliance with this standard is called PCI Compliance. PCI compliance, is officially known as the Payment Card Industry Data Security Standard (PCI DSS). Merchants that accept cards are mandated by their card acquirers to comply with this standard.

Shopify[11], in their Best Practice Guide Everything You Need to Become PCI Compliant, states that becoming PCI DDS compliant is an increasingly important step in ensuring the security of customer's data. But when it comes to putting monetary values behind becoming PCI compliant, things get a bit tricky. They have managed to find the following numbers on the topic: Gartner[12] estimated that in 2007, the nation's biggest merchants spent around $125,000 each assessing the scope required for PCI-related work, plus another estimated $568,000 to meet the requirements. Merchants with 1 to 6 million transactions per card type spent in the ballpark of $105,00 for scoping and $267,000 for compliance. And merchants with 20,000 up to 1 million transactions per card type expected to spend between $44,000 on scoping and $81,000 for compliance.

A newer study by the Ponemon Institute[13] in 2010, found that the largest merchants are paying on average $225,000 for compliance-related work and that 10% of the largest ones are paying $500,000 or more annually. Again, these are "on average" numbers. So, the costs involved will vary greatly from company to company but are not to be underestimated.

Issuing banks are deploying a variety of techniques and staff in order to protect cardholders against card related fraud. Technologies used are getting more and more sophisticated and nowadays machine learning technology is entering the bank's back offices. This modern technology comes with a price attached to it but it should help banks improve fraud detection, reduce false positive rates and increase fraud case handling efficiencies.

11 https://www.shopify.com/enterprise/86366534-everything-you-need-to-become-pci-compliant

12 https://www.braintreepayments.com/blog/what-does-it-cost-to-become-pci-compliant/

13 http://www.ponemon.org/local/upload/file/PCI%20DSS%20Trends%20-%20QSA%20Insights%20010310.pdf

Data breaches

Over 4.8 billion personal records have been exposed since 2013.

Data breaches are more and more common. In the majority of cases they involve theft of credit card details: on April 20th, 2011, the headlines read, "Sony PlayStation Network hacked, again. 77 million accounts compromised". On December 18th, 2011, newspapers reported "Target victim of a massive data breach, data from 40 million credit cards stolen", and on October 23th, 2015, "TalkTalk hacked by a group of 15-year-olds, data of 4 million customers breached". More recent high profile examples include the breaches of Ashley Madison (2015, more than 25 gigabytes of company data, including user details, was compromised) and Yahoo! (2014, but disclosed by Yahoo! in 2016), over 500 million user accounts were compromised).

Gemalto is tracking data breaches via their Breach Level Index. The Breach Level Index is a global database that tracks data breaches and measures their severity based on multiple dimensions, including the number of records compromised, the type of data, the source of the breach, how the data was used, and whether or not the data was encrypted. By assigning a severity score to each breach, the Breach Level Index provides a comparative list of breaches, distinguishing data breaches that are not a serious threat versus those that are truly impactful.

In their Breach Level Index update over the first half of 2016[14], Gemalto reveals that data breaches increased 15% in the first six months of 2016 compared to the last six months of 2015. Worldwide, there were 974 reported data breaches and more than 554 million compromised data records in the first half of 2016, compared to 844 data breaches and 424 million compromised data records in the previous six months. In addition, 52% percent of the data breaches in the first half of this year did not disclose the number of compromised records at the time they were reported.

According to the Breach Level Index, more than 4.8 billion data records have been exposed since 2013 when the index began benchmarking publicly disclosed data breaches. For the first six months of 2016, identity theft was the leading type of data breach, accounting for 64% of all data breaches, up from 53% in the previous six months. Malicious outsiders were the leading source of data breaches, accounting for

14 http://breachlevelindex.com/data-breach-library

69% of breaches, up from 56% in the previous six months.

In terms of the types of data breaches that were reported in the first half of 2016, identity theft was clearly dominant. The next most common type of attack was Financial access, as can be derived from the update. Both types of data breaches can be exploited to make fraudulent payments.

Regulatory Compliance

Mauritius has more government officials working on Anti-Money. Laundering implementation than the country has opticians.

Regulators have imposed all kinds of measures upon the payments industry that can be grouped under the header of compliance, and that have been introduced to make life of criminals and terrorists more difficult.

Compliance measures need to be implemented during the client on-boarding process (CDD and KYC) and on-going measures need to be implemented for transaction monitoring. Sanction screening needs to be performed against lists that are subject to change, and transactions need to be monitored for unusual patterns or sanctioned counterparties. Compliance requirements are also subject to change. Actors in the payments industry need to be continuously at par with latest requirements from local and foreign regulatory requirements.

All this comes at a price. Anti-Money Laundering (AML) efforts still cost money: an estimated $7 billion annually in the U.S. alone for implementing AML regulations from the international Financial Action Task Force (FATF). The cost is disproportionately more in smaller countries such as Mauritius, which has 1.3 million people and 25 government officials working on AML implementation — more AML bureaucrats than the country has opticians — and that's not counting bank staff who carry out customer investigations[15].

Not implementing the required compliance measures in a proper matter is not an option as a bank in the UK found out recently[16]: the bank was fined with GBP 3.25 million and the bank was also imposed a restriction, preventing it from accepting deposits from new customers for 168 days. The Financial Conduct Authority found serious and systemic weaknesses affected almost all levels of its AML control and governance structure, including its senior management team, its money laundering reporting function, the oversight of its branches and its AML policies and procedures. This meant that the firm failed to comply with its operational obligations in respect of customer due diligence, the identification and treatment of politically exposed persons, transaction and customer monitoring and making suspicious activity reports.

Failed transactions

68.81% of online shopping carts are abandoned before checkout. Payment is an important factor behind this.

The number of merchants (millions), acquirers (hundreds) and issuers (thousands) communicating via a number of card networks (around ten major networks), gives an indication of the amount of parties (and thus systems) communicating with each other in the complete payment ecosystem. All the parties, divided over different geographical regions (and jurisdictions) with different norms, values and interests, introduce a social complexity. All the systems, and their mutual interfaces and dependencies, introduce technical complexity and potential points of failure. The effect of this social and technical complexity also manifests itself in the authorisation phase of the payment process. Issuers can refuse a payment in their own interest and leave other parties in the dark about the reason. This is referred to as information asymmetry. Because of this information asymmetry other parties in the network are powerless to argue or act on the issuer's authorisation decision[17].

PayPal Froze My Account After I Bought a Cuban Cigar[18]

PayPal still seems to be interested in cracking down on the consumption of Cuban goods. On a recent trip to Tijuana, a friend bought me a Cuban cigar and I paid him back over PayPal. Shortly thereafter I received an email from PayPal saying that my account had been flagged for my possible promotion of transactions of goods prohibited by the U.S. government. I followed the instructions in the email and filed a report explaining that my purchase was made outside of the U.S. and

15 http://www.pymnts.com/news/2015/the-global-cost-of-anti-money-laundering-efforts/

16 https://www.finextra.com/pressarticle/66552/fca-slaps-325-million-fine-on-sonali-bank-for-aml-failings

17 Van Der Valk, R.J.A., 'Why My Payment Got Rejected: A Method to Mine Payment Refusal Clues', Master Thesis Delft University of Technology, 1st December, 2015, available at: http://repository.tudelft.nl/islandora/object/uuid:9768c196-e490-4ad7-b9e1-0912c5eb-f6a4?collection=education

18 http://www.forbes.com/sites/nathanielparishflannery/2016/08/18/paypal-froze-my-account-after-i-bought-a-cuban-cigar/

that I consumed the cigar while in Mexico. I received a follow-up email explaining that my account had been frozen.

Transactions can also fail to due increased scrutiny of fraud checks. And although it is good to know that most fraud attempts are being blocked by the fraud protection systems of the card industry, one of the side effects is that this increased scrutiny is resulting in so-called false positives, where genuine transactions are being flagged as possibly fraudulent. In the best case, these transactions are paid for by other means (cash or another card), but in the worst case the transaction will not be completed at all, which results in lost turnover for merchants as well as reputational damage.

Adele Reveals Her Credit Card Was Declined at an H&M Store: 'I Was Mortified'[19]

Even Adele runs into banking issues from time to time. The 28-year-old singer has been pretty candid about her adventures during her sold-out world tour, and in a recent concert, revealed that her credit card was actually declined at an H&M store in San Jose, California.

"I went to H&M and my card got declined. Oh my days, pretty embarrassing," Adele told the audience, according to The Mirror. "Nobody knew it was me, but I was mortified."

The Baymard Institute[20] analysed 34 different studies containing statistics on e-commerce shopping cart abandonment and concluded that there is a 68.81% – average documented online shopping cart abandonment rate. Looking at the reasons for shopping card abandonment, according to Statista[21], 18% of respondents indicated that they left the shopping process due to excessive payment security checks, and 17% of respondents had concerns about payment security. 11% of respondents indicated that their payment got declined.

For consumers it is quite embarrassing if card transactions are being declined by such fraud detection system, and unfortunately these systems are not discriminating based on card owners as the following anecdotes will tell.

19 http://www.etonline.com/news/194981_adele_reveals_her_credit_card_was_declined_at_an_hm_store/

20 http://baymard.com/lists/cart-abandonment-rate

21 https://www.statista.com/statistics/232285/reasons-for-online-shopping-cart-abandonment/

Obama's credit card declined at fancy restaurant[22]

Ever had your credit card turned down at a fancy restaurant? President Obama can commiserate. Speaking to workers at the Consumer Financial Protection Bureau in Washington on Friday, he recalled a moment last month when, at the end of a dinner out in New York City, his plastic was declined. "I guess I don't use it enough, so they thought there was some fraud going on," he said. "Luckily, Michelle had hers. I was trying to explain to the waitress that I've really been paying my bills".

Outages and breakdowns

In 2013, the Belgian card scheme broke down a few hours before Christmas.

Electronic payments rely on multiple parties and infrastructures and failure of one element in the whole transaction chain can block the ability for merchants to accept card payments.

On 23 December 2013, just before Christmas, the Belgian merchant community faced an outage of Worldline, the processor for the Belgian domestic debit card scheme Bancontact. The outage lasted for two and a half hours, and according to the Belgian Neutral Syndicate of Independents (NSZ), this outage costed Belgian retailers EUR 51 million in sales[23]. Smaller outages of Worldline have happened since as well[24].

On 24 May 2016, Switzerland's largest telecom provider, Swisscom, experienced a nationwide disruption to its network: cash appeared to be the only payment method that was still up and running. As a result, a large number of ATM machines were down in the cities of Lausanne and Zurich, while shopkeepers and retailers all over Switzerland were unable to accept card payments. The network failure lasted a few hours and went as far as causing Swisscom's cable and IP phone services to be down. The 3G and 4G mobile phone networks were unaffected.

During 2016, UK payment processor Worldpay was facing criticism as a part of its customers – mainly e-commerce and gambling websites – have had their payments system blocked during three weeks. The

22 http://edition.cnn.com/2014/10/17/politics/obama-credit-card/

23 http://www.hln.be/hln/nl/942/Economie/article/detail/1827811/2014/03/24/Kerstpanne-Bancontact-zelfstandigen-krijgen-5-miljoen-euro-compensatie.dhtml (in Flemish)

24 http://www.nsz.be/nl/zoeken?form=search&q_widget=worldline&submit= (in Flemish)

Issues and Compliance Measures in Payments

Money Laundering

Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origin. More precisely, it may encompass three distinct, alternative acts: (i) the conversion or transfer, knowing that such property is the proceeds of crime (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; and (iii) the acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime.

Financing of Terrorism

Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense within the scope of the Convention.

AML and CTF (Anti-Money Laundering and Combating the Financing of Terrorism)

Similar methods are used for both money laundering and the financing of terrorism. In both cases, the actor makes an illegitimate use of the financial sector. The techniques used to launder money and to finance terrorist activities/terrorism are very similar and in many instances identical. An effective anti-money laundering/ counter financing of terrorism framework must therefore address both risk issues: it must prevent, detect and

punish illegal funds entering the financial system and the funding of terrorist individuals, organizations and/or activities. Also, AML and CFT strategies converge; they aim at attacking the criminal or terrorist organization through its financial activities, and use the financial trail to identify the various components of the criminal or terrorist network. This implies to put in place mechanisms to read all financial transactions, and to detect suspicious financial transfers.

The international standard for the fight against money laundering and the financing of terrorism has been established by the Financial Action Task Force (FATF), which is a 33-member organization with primary responsibility for developing a world-wide standard for anti-money laundering and combating the financing of terrorism. The FATF was established by the G-7 Summit in Paris in 1989 and works in close cooperation with other key international organizations, including the International Monetary Fund (IMF), the World Bank, the United Nations, and FATF-style regional bodies.

KYC and CDD (Know Your Customer and Customer Due Diligence)

Many of the methods applied by criminals to launder money or finance terrorism involve the use of the financial system to transfer funds. Financial institutions, in particular banks, are most vulnerable to abuse for that purpose. In order to protect themselves, it is essential that financial institutions have adequate control and procedures in place that enable them to know the person with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls.

The application of strict Customer Due Diligence (CDD) by financial institutions and a high degree of transparency is crucial to fight money laundering and the financing of terrorism effectively. CDD must be applied upon establishment of a business relationship or in preparation of a specific cash transactions in excess of a certain amount. CDD must also be applied whenever financial institutions suspect money laundering or terrorist financing activities.

The basic steps of CDD measures are the appropriate identification of a customer and/or beneficial owner, the verification of the identity of the customer or beneficial owner, as well as the collection of information on the customer's purpose and nature of the business relationship.

International Standards on CDD have been set by both the Basel Committee on Banking Supervision (Basel Committee) and the Financial Action Task Force (FATF).

breakdown caused processing issues to only 1% of Worldpay customers, especially sports betting website Stan James and vintage e-commerce Etsy, but this outage could be enough to damage the reputation of the newly public company. Indeed, its stock price collapsed by more than 3.5% over two weeks. Worldpay declared that the problem arose from new software and system changes on the network and that only one of its servers was impacted. They reported the outage to the Financial Conduct Authority. The consequences could have been worse as Worldpay's client portfolio includes British Airways and the National Lottery.

Another reputational hit was taken by sponsor Visa during the Olympic Games in London in 2012. Members of the public were told at the national stadium that they could not pay by Visa, which was the only credit or debit card accepted at Olympic venues, and could only use cash. Spectators complained this led to massive queues and a lack of cash machines at the famous stadium also contributed to the problems. A spectator mentioned that he asked if there were any cash machines and he was told some had been taken out for the Olympics.

Other costs: e.g. environmental costs of bitcoin

Bitcoin consumes as much energy as Ireland.

Critics of cash often cite environmental concerns as one of the reasons why digital payment methods are "greener", but they fail to look beyond false appearances.

A study by the National University of Ireland[25] found that the bitcoin network's energy consumption was probably equal to that of all of Ireland, around 3 GW. This was in 2014. What would happen if bitcoin became a more universal payment method? Fabrice Flipo and Michel Berne[26] estimate that the monetary mass in circulation today is equal to 11 billion dollars. If that were all in bitcoins, it would require over 4,000 GW of energy to power them - or twice the energy consumption of the entire United States.

Processing bitcoins also requires a large financial investment. The processing cost of each bitcoin is USD 60, even when the environmental conditions are favourable and the data centres' energy costs are low (as in Iceland).

3. Comparison with Costs of Cash

In 2012 the ECB[27] carried out a study of the social and private costs of different payment instruments with the participation of 13 national central banks in the European System of Central Banks (ESCB). It shows that the costs to society of providing retail payment services are substantial. On average, they amount to almost 1% of GDP for the sample of participating EU countries. If the sample results from the participating countries were extrapolated to 27 EU Member States, the social costs of retail payment instruments are being close to €130 billion. Half of the social costs are incurred by banks and infrastructures, while the other half of all costs are incurred by retailers. The social costs of cash payments represent nearly half of the total social costs, while cash payments have on average the lowest costs per transaction, followed closely by debit card payments. However, in some countries, cash does not always yield the lowest unit costs.

The European Commission's Report[28], the "Survey on merchants' costs of processing cash and card payments", found that the marginal cost of cash appears to be higher than the marginal cost of (debit or credit) card if the MSC (and hence the interchange) component is excluded. However, if the MSC cost component is included, the current marginal costs of (debit or credit) card exceed the marginal cost of cash per transaction. Therefore, whenever a consumer decides to use a card instead of cash to make a payment, on average the merchants surveyed suffer a negative externality due to an excessive MIF level. That means that the merchants in the sample would be better off, on average, if the transactions currently executed with card were carried out by cash. That implies that the MSCs and therefore the MIFs are currently on average above the indifference threshold for the surveyed merchants.

Conclusion

The reports from the European Commission and the European Central Bank as quoted before have been based on sound research, but have taken only the visible costs of card payments into account. Even whilst

25 "Bitcoin Mining and its Energy Footprint", Karl J. O'Dwyer and David Malone, available at: https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf

26 http://rue89.nouvelobs.com/2016/07/20/bitcoin-block-chain-gouffres-energetiques-264719 (in French)

27 ECB, "The social and private costs of Retail Payment Instruments, a European Perspective, 2012, available at https://www.ecb.europa.eu/pub/pdf/scpops/ecbocp137.pdf

28 http://ec.europa.eu/competition/sectors/financial_services/deloitte_payment_acceptance_survey_en.pdf

only looking at those visible costs, the ECB found that the social costs of cash payments represent nearly half of the total social costs, while cash payments have on average the lowest costs per transaction.

In this paper a plethora of other less visible cost items for card transactions have been identified. Although the scope of this paper was limited to identifying those costs, it goes without saying that if these hidden costs would be quantified it would add significantly to the cost of card payments.

Regardless of the actual bearer of the costs identified in this paper, the participants in the card payments value chain will always take these costs into account whilst setting their pricing towards the end-users of their services. Most likely, as a result of this, the consumers and the tax-payers are picking up this bill.

4. Glossary

Term	Meaning
Acquirer, Acquiring Bank	The bank of the merchant. In point-of-sale (POS) transactions, the entity (usually a credit institution) to which the acceptor (usually a merchant) transmits the information necessary in order to process the card payment.
Card Scheme	A technical and commercial arrangement set up to serve one or more brands of card which provides the organisational, legal and operational framework necessary for the functioning of the services marketed by those brands.
Card Scheme Fee	A Fee that banks need to pay to the card scheme for using the brand of those card schemes.
EMV	EMV is a technical standard for smart payment cards and for payment terminals and automated teller machines that can accept them. EMV cards are smart cards (also called chip cards or IC cards) which store their data on integrated circuits rather than magnetic stripes, although many EMV cards also still have magnetic stripes for backward compatibility. Payment cards that comply with the EMV standard are often called chip-and-PIN or chip-and-signature cards, depending on the exact authentication methods required to use them. EMV stands for Europay, MasterCard, and Visa, the three companies that originally created the standard. The standard is now managed by EMVCo (http://emvco.com/), a consortium with control split equally among Visa, Mastercard, JCB, American Express, UnionPay, and Discover.
Identity Fraud, Identity Theft	Identity theft is when personal details are stolen and identity fraud is when those details are used to commit fraud.
Interchange Fee, Multilateral Interchange Fee (MIF)	A transaction fee payable between the payment service providers involved in a transaction. In card transactions this fee is paid by the Acquirer to the Issuer.
Issuer, Issuing Bank	The bank of the cardholder. A financial institution that makes payment cards available to cardholders, authorises transactions at point-of-sale (POS) terminals or automated teller machines (ATMs) and guarantees payment to the acquirer for transactions that are in conformity with the rules of the relevant card scheme.
Merchant Service Charge (MSC)	The fee that a merchant must pay to his Acquiring Bank for accepting the card as a means of payment.
Processing Fees	Fees that banks need to pay for the authorisation, clearing and settlement of card transactions.

5. Bibliography

- 'Global Payments 2016 – Competing in Open Seas', the Boston Consulting Group; September 26, 2016; Stefan Dab, Mohammed Badi, Laurent Desmangles, Alenka Grealish, Federico Muxi, Bharat Poddar, Olivier Sampieri, Yann Sénant, and Pieter van der Berg.
- 'World Payments Report 2016', BNP and Capgemini
- 'Cash Essentials - Beyond Payments'; 2016; Guillaume Lepecq; http://www.cashessentials.org
- 'Multilateral Interchange Fees: Competition and Regulation in light of Recent Legislative Developments', January 2014, Maria Chiara Malaguti and Alessandra Guerrieri; European Credit Research Institute (ECRI).
- 'Fourth Report on Card Fraud', July 2015, European Central Bank

6. About the Authors

Diederik Bruggink is an International Expert in Payments, Cards and Market Infrastructures and has been active in the payments business since 1999. Since 2012, he is an independent consultant.

He has worked within or completed strategic assignments at key companies in Cards, Payments and Transaction Banking such as The Royal Bank of Scotland, WorldPay, ABN AMRO, MasterCard, Capgemini, ING, OP Bank, International Card Services, Equens (predecessor Interpay), TSYS, Eufiserv, Vodafone (predecessor Libertel), SafetyPay, Ingenico ePayments (formerly Global Collect), Monnet (EU Bank initiative to create a new European payment card scheme), Efma and Tranwall. His expertise focuses on business strategy, proposition and business process issues, and he has undertaken for example: international payments strategy, partner selection processes and market entry studies.

Diederik holds a Master Degree in Mechanical Engineering from the University of Twente in the Netherlands. He is a Dutch citizen and lives in Belgium.

Diederik was one of the key authors of the first three editions of the World Payments Report, and he makes regular appearances on conferences in the cards and payments industry. He is a member of the Editorial Board of the Journal of Payments Strategy & Systems as well as a regular contributor to this Journal.

Guillaume Lepecq is a globally recognized expert in retail payments and cash. Working primarily as a consultant over the last fifteen years, Guillaume also worked for Brink's Europe, Middle-East and Africa (EMEA) as Vice-President of Money Processing where he was responsible for leading the development efforts for integrated money processing solutions for financial institutions and retailers.

He has spent the last ten years advising financial institutions throughout Europe on their payment strategies and has been involved in wide-scale projects related to European financial integration, such as the euro cash changeover, the migration to EMV cards and the implementation of the Banknote Recycling Framework.

From 1993 to 2001, Guillaume was Director of Corporate Relations at the Association for the Monetary Union of Europe, a business lobby and think-tank backing Economic and Monetary Union.

Guillaume is also a published author, who has written a number of publications and reports detailing the role of cash and payments in society including: "Cash Essentials – Beyond Payments", "The Future of Cash", "The Future of Smart Payments" and the "Managing the Changeover to the Euro".