IANUS
Diritto e Finanza
UNIVERSITÀ DI SIENA 1240
Quaderni
https://www.rivistaianus.it
ISSN: 1974-9805
Quaderni - 2015

MODULO JEAN MONNET

END-TO-END ENCRYPTION IN ON-LINE PAYMENT SYSTEMS: THE INDUSTRY RELUCTANCE AND THE ROLE OF LAWS

Safari Kasiyanto

END-TO-END ENCRYPTION IN ON-LINE PAYMENT SYSTEMS: THE INDUSTRY RELUCTANCE AND THE ROLE OF LAWS

Safari Kasiyanto
PhD researcher, Tilburg Law and Economic Centre (TILEC)
Junior research fellow, European Banking Centre (EBC), Tilburg University
Legal advisor, Bank Indonesia (the central bank of Republic of Indonesia)

Various security breaches at third-party payment processors show that online payment systems are the primary target for cybercriminals. In general, the security of online payment systems relies on a number of factors, namely technical factors, processing factors, and legal factors. The industry gives its best endeavours to strengthen the technical and processing factors, while the government has been called upon to improve the legal factors. However, a breach of consumer's data and financial losses resulting from such a breach keep occurring. Findings from the forensic audit show that most online payment systems, such as those using credit and debit cards as their instruments, have a weak point leaving the systems vulnerable to hacking. This weak point concerns the so-called financial data in transit that are not fully encrypted. Encryption is indeed employed within the systems, but only on certain networks. Industry's standard reflected by code of conducts only obliges the players to encrypt the financial data transmitted on the public network, and not on their private networks. On top of that, laws and regulations are often in a vacuum to regulate the encryption. Thus, although seen as the strongest method so far to prevent the breach, end-to-end encryption has not entirely been implemented. Why does the industry seem to be reluctant in implementing end-to-end encryption? What do laws rule on this and would it be appropriate for the law to rule such obligation for the sake of consumer protection? This paper tries to shed a light on these issues. To investigate the industry reluctance, this paper discusses security of online payment systems and the nature of the retail payment systems. As for the laws and regulatory frameworks, this paper outlines and focuses on the EU level. Online payment systems using credit or debit cards are used as the main example in this paper as such methods have much more matured compared to the others. However, special attention on the innovative payments such as mobile payments and virtual currencies will be drawn as the security issues of such innovative payments have given rise to regulatory challenges.

Table of Content

1.Introduction
2.What are Online Payment Systems?
3.Security of Online Payment Systems
4.Breaches in Online Payment Systems
5.Improving the Security of Online Payment Systems
  5.1 Chip and PIN
  5.2 Tokenization
  5.3 Quantum Secure-Authentication
  5.4 End-to-End Encryption
6.End-to-End Encryption: Why it has not been Implemented

6.1 Economic Reasons
6.2 The Design of Online Payment Systems
6.3 The Nature of Retail Payment Systems
7.The Role of Laws
7.1 Payment System Directive
7.1.1 Provision applicable for implementing encryption
7.1.2 Does the framework suffice?
7.1.3 Among the hype of innovative payments
7.2 Proposal of Payment System Directive 2 (PSD 2)
7.3 Other Regulatory Frameworks
7.3.1 Data Protection Directive
7.3.2 Privacy and Electronic Communication Directive
7.3.3 Encryption law
8.Conclusion
References

1. INTRODUCTION

In the last decade various security breaches occurred all over the world, putting consumer personal data in jeopardy. These breaches, in particular those occurring at third-party payment processors, show that online payment systems are the primary target for cybercriminals. Although trend on financial losses from breaches is quite steady, trend on the compromised data from the same breaches is increasing[1]. Breaches that occurred at payment processors such as Heartland Payment System and others such as the US Office of Personnel Management, Kaspersky Lab and BlueCross, involved hundreds of millions of data, serve as a wake-up call: online payment systems are vulnerable and need to be secured.

In general, the security of payment systems relies on a number of factors, namely technical factors, processing factors, and legal factors. The industry gives its best endeavours to strengthen the technical and processing factors[2], while the government has been called upon to improve the legal factors. However, a breach of consumer's data and financial losses resulting from such a breach keep occurring.

Findings from the forensic audit show that most online payment systems, such as those using credit and debit cards as payment instruments, have a weak point leaving the systems vulnerable to hacking[3]. This weak point exists when financial data are in transit, while not being fully encrypted. In this circumstance encryption is indeed employed within the systems, but only on certain networks. Industry standard reflected by code of conducts and often byelaws only oblige the payment providers to encrypt the financial data transmitted on the public network, and not on their private networks. On top of that, laws and regulations are often in a vacuum to regulate the encryption. Thus, although seen as the strongest method to prevent a breach, end-to-end encryption has not been fully implemented.

This paper tries to shed a light on the following issues:

- Why does the industry seem to be reluctant in implementing end-to-end encryption?
- What is the role of the existing laws to strengthen the security of online payment systems?

---

[1] Cheney, 2010.

[2] For example, in card payments the industry has an agreement to apply a technical standard, namely the Payment Card Industry Data Security Standard (PCI DSS).

[3] One excellent example is a breach occurring at a third party payment processor in the US, Heartland Payment System that will be discussed further in the later subchapters.

In seeking the answers, this paper will discuss the security and design of online payment systems and the nature of retail payment systems.

It is worth noting that in this paper, online payment systems using credit/debit cards are used as the main example regardless the delivery channel they use, whether they use the Internet (internet payments), mobile device (m-payments), ATM or Point of Sales (POS) terminal (card payments) to initiate payment orders. However, special attention on the innovative payments in particular m-payments and virtual currencies will be drawn as the security issues of such innovative payments have given rise to regulatory challenges. As for the laws and regulatory frameworks, this paper will outline and focus on the EU level. Methodology employed for this paper is legal research with law, technology and economic approaches. In this manners, the relevant EU directives with focus on payment system directive are analysed for any loopholes in light of the business practices.

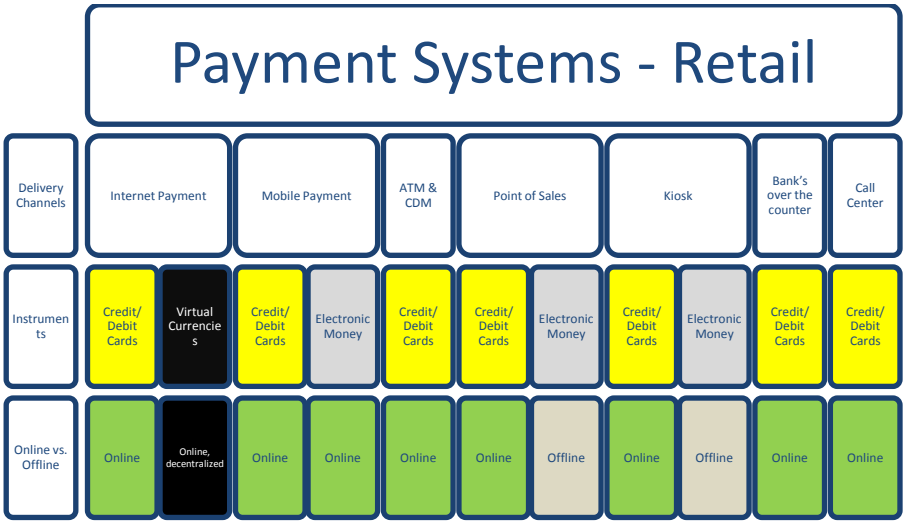
This paper is structured as the following. Section 2 briefly overviews what are online payment systems discussed in this paper, their examples and limitation. It follows by discussions on the security of online payments in Section 3 and breaches occurred in online payments in Section 4. Section 5 elaborates on how to improve the security to prevent such breaches occurred in the future. Analyses are provided in Section 6 and 7, discussing the reasons why end-to-end encryption has not been fully implemented and what is the role of laws, respectively. It ends with conclusion provided in Section 8.

2. WHAT ARE ONLINE PAYMENT SYSTEMS?

There are some confusions when it comes to the definition and scope of online payment systems. Among non-professionals, an online payment system is understood as any system that enables payments to be made through the Internet only. Although not false, this definition is not entirely correct. The professionals in payment systems employ some well-accepted terms such as Gross vs. Net systems, Large-value vs. Retail, as well as Online vs. Offline systems. Among such professionals, an online payment system means any system that requires access to the central server to authenticate a payment order for authorization. Here, access to the central server does not necessarily imply the use of the Internet, but can also be done through a private network. As example of online payment are any transactions made by a consumer using credit or debit cards at a store or

through the Internet, m-payments using an app or telecommunication network to initiate transactions and most of virtual currencies.

By contrast, offline payment systems do not require access to the central server to authenticate the payment order. Thus, transactions processed through offline systems can be, and should be, done locally, usually involving an instrument such as a smart card and a reader device. Settlement to the central database is usually done in bulks by the end of the day or in the next day of the transactions. As an example of offline payment is transactions made using a store-value card (also known as electronic money) for transportation services such as buses or trains and m-payment using Near Field Communication (NFC) technology.

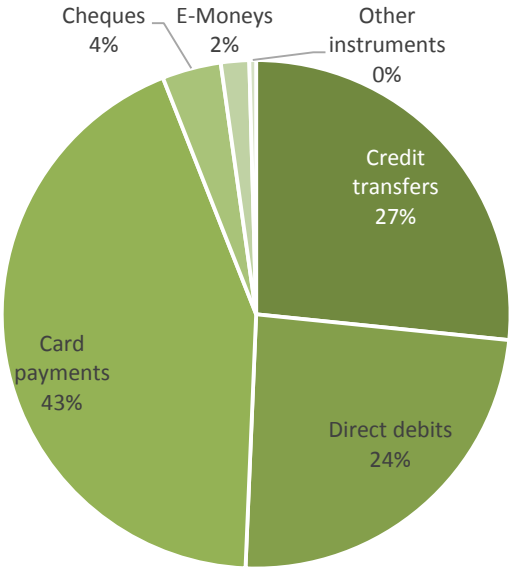


Source: Author.

Figure 1 Retail Payment Systems: Delivery Channels, Instruments and Online vs. Offline

As shown in figure 1, retail payment systems encompass a number of delivery channels such as the Internet, mobile phone, Automated Teller Machine (ATM) & Cash Deposit Machine (CDM), Point of Sales (POS) at merchants or shops, kiosk, bank's branch and call centre. Regardless the delivery channel a consumer uses, the transaction will require an instrument. Broadly speaking, payment instruments mainly consist of three instruments: paper-based (such as checks), card-based (such as credit/debit cards), and electronic-based (such as e-money and virtual currencies, and later on

crypto-currencies[4]). The focus of this paper is online systems no matter the delivery channels or instruments they use. However, online payments made using credit/debit cards might appear more in the analysis as such systems are the most mature compared to others[5] (see figure 2[6]). Specific attention on online m-payments and virtual currencies will be drawn as the security issues of such innovative payments have given rise to regulatory challenges.



Source: ECB, Payment System Statistic[7]

Figure 2 Percentage of the use of payment instruments in the EU in 2013 based on number of transactions

[4] There is no doubt that crypto-currencies such as Bitcoin is electronic-based as it is basically a computer file encrypted with a unique logarithm using public and private key for authentication prior a transaction. For detail see for instance European Central Bank, *Virtual Currency Scheme*, 2012. Pay attention on the elaboration of Bitcoin as a case studies, page 21-27.

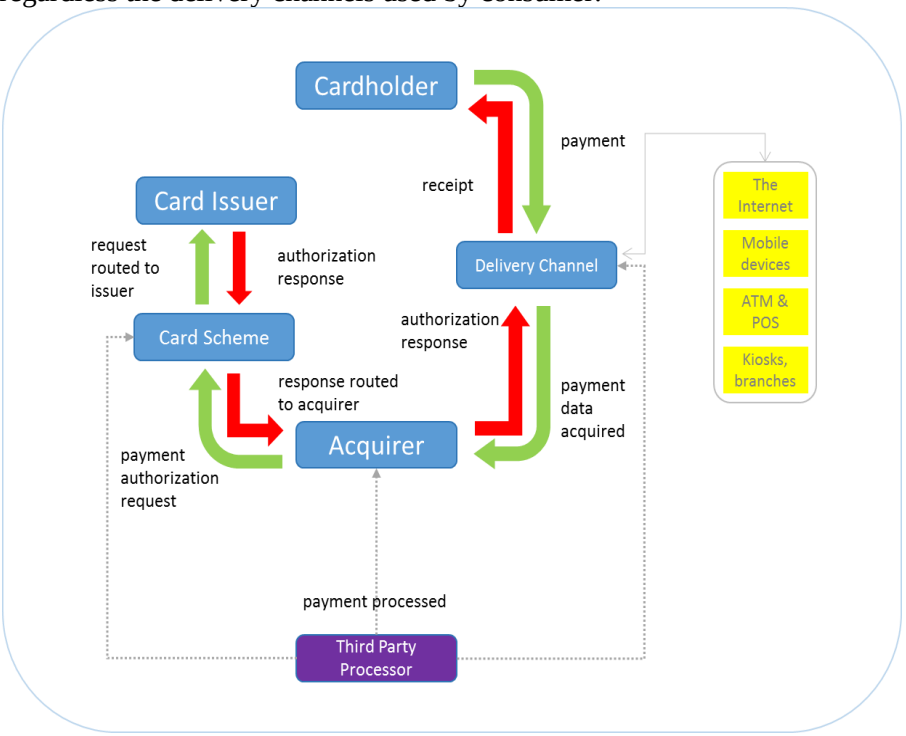
[5] For an excellent discussion on the significance of card payments, see for instance Borestam and Schmiedel, 2011: 8-9.

[6] Unfortunately, both m-payments and virtual currencies have not been included in the figure as the existing statistic provided by ECB does not make any distinction to these types of payment systems/instruments.

[7] www.ecb.europa.eu/stats.

3. SECURITY OF ONLINE PAYMENT SYSTEMS

Before discussing the security of online payment systems, we need to outline how a transaction is processed through online payments. Therefore, a general model of online payment systems needs to be set. Although generated from online transactions made using credit/debit cards, the general model as shown in figure 3 could be applied to all types of online systems regardless the delivery channels used by consumer.



Source: www.theukcardsassociation.org.uk, modified and adjusted[8].

Figure 3 General Model of Online Payments using Debit/Credit Cards as Instruments

From such a general model, one can draw three important elements in online payment systems that have a direct influence to the security employed: instruments used to initiate payments, delivery channels, and the

[8] See also basic flow chart in Borestam and Schmiedel, 2011: 10. Pay attention in particular on business model of four-party scheme.

networks. Bearing in mind these three elements, the security employed in online payment systems is as the following.

The first one deals with the security of the payment instruments. As described in subsection 3, cards are the most common instruments used in online payments (see figure 2). Security employed in card instruments is generally as the following. When first time introduced in around 1950s[9], credit cards used magnetic stripe technology. This technology was still used in most countries until 2008 when the card scheme started introducing smart card technology. In fact, magnetic stripe cards are still used mainly in the US today[10]. The case of debit cards is the same, following credit card systems as their predecessor. In the beginning, debit cards also used magnetic stripe technology but then gradually replaced by smart cards.

Security used in magnetic stripe cards is considered as the lowest[11]. They only have ability to store card data such as card digit number and expiry date used for personalisation. They have no ability to encrypt or decrypt and barely no security at all. When a cardholder swipe his or her magnetic stripe cards, the data stored in the magnetic stripe technology is sent to the terminal for validation and then, assuming the data is valid, to the issuer for authentication. The data processed consists of bare digit numbers that are easy to clone. In this manner, magnetic stripe cards are vulnerable for fraudulent. There were so many cases where skimmed and cloned cards were used by fraudsters.

The second issue is the security of the delivery channels. Some delivery channels are more mature and highly regulated, while some others are new and less- or un-regulated. The first includes ATM and POS terminals owned by banks that highly regulated under financial sector, while the latter includes the Internet and mobile device. Recent research shows that mobile devices are, for instance, vulnerable from *phishing* or *shmishing* (attack via short messages), malware and reckless users (lost and stolen device, public WIFI usage or weak passwords) as such devices are made for telecommunication function and not for conducting payments.

The last issue deals with the security employed for the networks. Until recently, there is neither an explicit law nor a standard agreed by all providers to employ a certain level of security for networks. As for the law, the European Commission introduced a proposal to regulate security of

[9] Schmalensee and Evans, 2005.
[10] Accounted for approximately 90% of the total cards by the end of 2014.
[11] Turban and Brahm, 2000: 282.

network and information[12], whereas for industry standard the most established standard is that of card payment industry[13]. Even within card payments, there was no use of any encryption technology in the beginning. After many cases of frauds (skimming, tampering and breaching) the industry started to inquiry encryption to be employed within the networks.

However, until currently industry standard only emphasizes the use of encryption technology for data at rest and data in transit within public networks. Since the existing requirement for employing encryption technology is still restricted to private network, data in transit through the public networks remains vulnerable to hacking.

4. BREACHES IN ONLINE PAYMENT SYSTEMS

This paper does not aim at providing an exhaustive list of the breaches but highlighting the breaches that relate to online payment systems, regardless the locus of the breaches. Skinner defines a security breach as "*a successful attack on a computer system's security controls in order to penetrate the system to acquire or corrupt information on the system, thus disrupting the confidentiality, integrity, or availability of information on the system"*[14]. This definition will serve as fundamental basis in outlining the relevant case of breaches.

The impact of security breaches to firms can be enormous in term of financial losses. The Computer Security Institute reported that in 2005, 639 of 700 respondents surveyed experienced breaches, costing such firms more than USD131 million in total, or in excess of USD 203 thousand per a firm in one single year only[15]. In addition, firms suffering the loss of sensitive data have also other financial shortfalls such as customer defections and decline in revenue and stock[16].

This significant financial loss impact also occurred to Heartland Payment System when a hacker interfered its network in late 2008, causing breach of

[12] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7 February 2013, COM(2013) 48 final, 2013/0027 (COD).

[13] The Payment Card Industry Data Security Standard (PCI DSS), available at https://www.pcisecuritystandards.org/security_standards/.

[14] Skinner in Rode, Lilia, 2006: 1604.

[15] Gordon et al., 2005.

[16] IT Policy Compliance Group, 2007: 4.

approximately 100 million debit/credit card data[17]. Heartland is the fifth biggest third party processor in the US, processing over USD80 billion and 4.2 billion transactions annually from more than 250,000 clients[18]. The breach occurred as an outsider succeeded in interfering Heartland's payment network, after about six months hiding his activities within the corporate network. Hartland's corporate network was first interfered with SQL injection, and then it moves from corporate network to payment processing network by installing sniffer software enabling to capture the payment data[19]. Hence, fraudsters breached Heartland by stealing data when they are being processed (in transit) within the private network and not from the database (at rest). After such accident, Heartland carefully reviewed the security employed in its systems and made steps to improve it, including a plan to employ end-to-end encryption.

5. IMPROVING THE SECURITY OF ONLINE PAYMENT SYSTEMS

Improving the security of online payment systems is not an easy task. Depending on the nature, format and design of each system, literature shows that currently there are at least four methods to improve the security of online payment systems. Each method has its own benefit and disadvantage in preventing a breach to occur, and is outlined and reviewed below. However, it is worth noting that these methods are continually evolving. What is considered as the safest method today might be no longer safe tomorrow.

5.1. Chip and PIN

The most well-known technical security to improve the use of debit/credit cards in online payments is the replacement of magnetic stripe cards with smart cards. The previous cards were used for debit/credit card transactions in the beginning up to several years ago. In fact, they are still used for most payments in the USA. By end of 2014, there were already more than 5.4 billion of smart cards used worldwide[20]. Laymen recognize this smart card technology as Chip and PIN.

---

[17] Lewis, 2015.
[18] Cheney, 2010: 2.
[19] Cheney, 2010: 3-4.
[20] EMVCO, *Worldwide EMV Chip Card Deployment*.

Basically, smart cards employ microprocessor chip to improve the security of magnetic stripe. This microprocessor provides several means of authentication to safely authorize transactions, mostly using cryptographic value. On EMV cards for instance, the security methods employed are cryptography called an Authorization Request Cryptogram (ARQC). Along with the transaction data, this cryptographic is sent to the card issuer for authorization. If the data is approved as valid data, the issuer then generates another cryptographic namely Authorization Response Cryptogram (ARPC). This method helps the card industry reduce transactions using counterfeit cards[21].

However, smart cards used in online payment systems only eliminate certain frauds such as those resulted from skimming and counterfeiting cards. These frauds are only valid for card-present transactions using magnetic stripe cards. For card-not-present transactions such as the Internet or mobile payments, the use of smart card technology is irrelevant as they do not require a physical instrument rather than a set of personal data to initiate a payment order.

5.2. Tokenization

Security used in tokenization is by generating random numbers to replace the payment data, and then sending such "tokenized" data to the third party processor. In this manner, retailers do not need to save or keep the "naked" payment data into their systems. All the payment data (and consumer data) are maintained and kept safely in the system owned by third party processor. Therefore, if a retailer or its system is tampered, fraudsters will not be able to capture the real data because they are not saved in the system of the retailer. This technology is highly relevant to secure transactions using the Internet payments and app-based mobile payment.

The flaw of this security improvement is that if a breach occurs at the third party processor, such as that happened to the Heartland Payment Systems in 2013, thieves are still enable to harvest all the data and use the compromised data to gain financial benefits. In this case, tokenization has no intended impact. That is why in many occasions tokenization is employed along with encryption.

[21] EMVCO, 2011: 89.

5.3. Quantum Secure-Authentication

Quantum secure-authentication uses proton of light to authenticate the confidentiality, integrity, and availability of information[22]. The method is complex, involving so-called physical unclonable function (PUF) as part of authentication process. The problem of this method of authentication is that this method has not been used in a real system. It seems flawless in laboratory but not yet tested in real life. Hence, it needs further research and a series of implementation stages to prove it robust.

5.4. End-to-End Encryption

General concept of end-to-end encryption is to encrypt both data in-transit and data at-rest. Data in-transit concerns the payment data that are being processed through the network, while data at-rest are data that are stored in the system database. Encryption of these data serves as an integral part of the authentication and authorization processes of payment instruction. Once end-to-end encryption employed, the payment data are no longer transmitted among the network participants in clear texts. Hence, the fraudsters who succeed to hack the system will unable to take advantage of the encrypted data. This technology can be employed for all types of online payment systems: internet payments, m-payments and card payments as basically it secures the three elements of online payments: instruments, delivery channels and networks.

However, there are two arguments when it comes to the starting point of encryption in end-to-end encryption[23]. The first one argues that by employing end-to-end encryption it means that the data should be encrypted once it has left consumer's devices, right after the consumer has initiated a payment order. On the other hand, the second argument believes that the data should already be encrypted within the device itself. This different arguments of end-to-end encryption's starting point lead to different tools for implementing encryption, the cost embedded, and the perceived security of the systems.

[22] Goorden et al., 2014: 421-424.
[23] Cheney, 2010: 9-10.

6. END-TO-END ENCRYPTION: WHY IT HAS NOT BEEN IMPLEMENTED

After carefully reviewing the relevant literature and scrutinizing the design of online payment systems, we argue that there are three main reasons on why end-to-end encryption technology has not been fully implemented. These reasons are economic reasons, the obstacles come from the design of online payment systems, and the difficulties arisen by the nature of retail payment systems.

6.1. Economic Reasons

For retail industry, the costs incurred by using payment instruments are not inexpensive. An empirical study by ECB in 2012 showed that the social costs for using payment instruments amounted to nearly 1% of GDP for EU member states[24]. While half of these social costs incurred by banks and payment infrastructure entities, 46% of such costs incurred by retailers. The remaining costs were shared between central banks (3%) and cash-in-transit companies (1%). As for the private costs, retailers also incurred the highest cost (at 0.587% of GDP), even compared to those of banks and infrastructures (at 0.493% of GDP) [25]. This is because retailers were exposed higher external fees to be paid to the payment providers. For instance, in some cases in the US some small retailers are even bound to a 48-month contract with acquirer to set-up POS terminals at their shops[26]. As for the Internet and app-based m-payments, costs incurred by retailers can be reduced as they do not need to set up terminals. However, NFC-based m-payment still requires to set-up POS terminals or to upgrade the existing terminals to enable m-payment transactions.

Implementing end-to-end end encryption will incur another cost to the retailers, and this cost is also not cheap. It could be a burdensome especially when it comes to small and medium retailers. Although retail industry in the EU includes some of the largest multinational companies, they are only a few. Over 95% of retailers in the EU are small and medium enterprises[27]. That is why this cost issue might be the main reason why the industry seems to be reluctant.

---

[24] Schmiedel et al., 2012: 6.

[25] Schmiedel et al., 2012: 25-26.

[26] DeSimone, 2015. See comments from some merchants in the US on this online article.

[27] European Commission, 2013: 7.

Taking into account on the different opinion of the starting point of end-to-end encryption previously discussed[28], there are two scenarios in calculating the cost for implementing end-to-end encryption. Whichever the scenario, both costs will consist of fee for software and hardware upgrades. The latter includes delivery channel upgrades when applicable (such as POS terminals and ATM). It is worth noting that the following calculations aim at providing an illustration only, on how implementing end-to-end encryption incurs a high cost.

Scenario 1 – encryption starting from the terminals

For scenario 1, cost for implementing end-to-end encryption 'only' consists of cost for employing encryption software and cost for upgrading the related hardware such as POS terminal and ATM & CDM. However, these costs cannot be considered as inexpensive. While cost for implementing encryption software may be considered relatively affordable, this is not the case for the cost of upgrading hardware. Hardware such as POS terminal and ATM have to be upgraded to have ability to read and communicate with encryption-enable instruments such as smart cards. After upgraded, this hardware will enable to authenticate whether a payment instrument is genuine or not.

Cost for upgrading the delivery channels can be enormous to be borne solely by one company. Let's take a look at the case of upgrading POS terminal and ATM. In this case (and in most cases), acquirer is responsible for such cost. However, the acquirer will then pass the cost to its merchants, the retailers. There is no way that a merchant gets all the terminals installed at their stores for free.

To give a real illustration on how much the cost incurred in upgrading terminals, let's take a look the number of terminals available within the EU countries. By 2013, there were in excess of 9 million POS terminals and more than 434 thousand ATMs available within the EU[29]. Taking into account that the modest cost for upgrading one POS terminal is in average of USD 300[30], and the cost for upgrading one ATMs is approximately USD 1400[31], the total cost for upgrading both POS terminals and ATMs would be

[28] See subsection 6.4.4 paragraph 2.

[29] European Central Bank, Payment System Statistics. Available at http://sdw.ecb.europa.eu/reports.do?node=1000004051.

[30] DeSimone, 2015. See also comments from some merchants, addressing on how much cost incurred to get a smart-card ready terminals fo thei stores.

[31] Payments Leader, *Will retailers be ready for EMV by Oct 2015?*

USD 2.7 billion and USD 607.6 million respectively. It is worth noting that vast majority of the merchants in the EU are SMEs, accounted for 95%. Such costs will be burdensome to those SMEs. However, it is also worth restating that this calculation is just a raw calculation for an illustration only. To have a real calculation on the cost, it needs to be meticulously investigated.

Scenario 2- encryption from the instruments

For scenario 2, cost incurred for the implementation of end-to-end encryption will be cost for scenario 1 + cost for replacement of cards. All cards that have no ability to encrypt and decrypt need to be replaced with smart cards. If one company considers that cost for scenario 1 is not cheap, cost for card replacement is even more expensive. For illustration, one magnetic stripe costs from USD 0.25 to USD 0.65 only, while cost for one smart card is much more expensive, ranging from USD 1 to USD 20[32]. Imagine, if there were in excess of 768 million cards[33] in the EU countries in 2003[34], it roughly needed at minimum of USD 268 million for the card replacement only.

6.2. The Design of Online Payment Systems

Unlike Systemically Important Payment Systems that process large-value payments and are mostly run by governmental body, most online payment systems are set up and run by private entities and using private networks. Therefore, it is not surprising at all that these entities are looking for profit in order to maintain their sustainability. As profitability is one of their main goals, these entities always meticulously apply cost and benefit calculation in pricing and investment, including when it comes to implementing security technologies. One might see this circumstance as a cause why it looks like that online payment systems slightly put security aside by, for instance, using magnetic stripe cards and unencrypted network for processing sensitive data.

Beside the fact that online payment systems were designed by private entities, consumer perception on security of online payment systems also play a significant role[35]. The systems will be widely accepted if consumers

[32] Turban and Brahm, 2000: 282-283.

[33] Cards with a cash function, based on ECB Payment System Statistics, 2013.

[34] ECB, Statistics on payment system instruments.

[35] See for instance Kim et al., 2010.

perceive security as sufficient, and *vice versa*. In the extreme condition it would not be an exaggeration to conclude that if industry gets an impression that the consumers perceive the existing security as sufficient, it might make the parties involved in such industry stop improving the security. To some extent, this role is a part of network externalities in payment systems, the wider network usage the better the systems run. Moreover, this role also supports the Schumpeter's theory that "economic logic prevails over the technological innovation". That is why we see sloppy wire hanging over the city rather than stainless cable. In the context of online payment systems, that is why we easily find low-security systems are in existence and even widely used.

Another factor is that rigid security may have an impact on the convenience of the user. In several cases, advance security requires an adept user and reduces the user friendliness. For instance, the use of longer PIN will make the user use more time to memorize it rather than shorter PIN, and the use of tokenization will require the user to follow some further steps tokenizing his or her PIN or personalised data, rather than just one click to initiate a transaction. This factor has a great impact on the design of online payment systems.

6.3. The Nature of Retail Payment Systems

As a part of retail payments systems, online payment systems share the same nature and characteristics of retail payments that may serve as one reason why it is not easy to implement an advance security such as end-to-end encryption. One notable nature is that online payments basically involve small monetary value transactions between consumers to business, or consumers to consumers in case of, for instance, P2P transfers. Payment providers need to focus more on the volume rather than value to get more benefits in providing such payment services. Hence, rapid and mass transactions could serve a key role in designing a potential system. This condition requires the payment providers to be more precaution in allocating resources, securing the profit that will maintain the sustainability of the business. The precautionary includes carefully calculating investment for IT in which security technology is part of it.

Another characteristic is that there are several, if not many, parties involved in online payment systems, from consumer, merchant, issuer of the instrument (if applicable), acquirer of the system to network owner to third party processor. This often leads to coordination problems among the participants of the systems. Problems include resource allocation such as

human resource and cost, as well as technical issues such as interoperability between different systems of participants. Take upgrading POS terminal in implementing end-to-end encryption as an example. Merchants, third party processors and acquirers need to sit down together to discuss the cost incurred and human resource allocation for upgrading process. As the number of retailers can reach hundreds of thousands or even millions in one country (in the EU for instance amounted to 3.6 million[36]), this negotiation can be very exhausted and time consuming.

7. THE ROLES OF LAWS

The existing law at the EU level that could serve as the legal basis for encryption are mainly the EU Payment System Directive (PSD). Thus, the main focus in this section will be the elaboration of the PSD, covering the existing and the proposed directive. However, some other laws such as Data Protection Directive, Privacy and Electronic Communication Directive and law on encryption will also be briefly discussed as they also contain some provision applicable to system security.

7.1. Payment System Directive

The PSD, which took into force on 1 November 2009, aims at achieving a comprehensive yet modern set of rules for all payment services available in the EU[37]. It covers all types of cashless payment services, including electronic and online payments, regardless any instruments they use[38]. By harmonizing the level of regulations, the PSD ensures that among the member states of the EU the electronic payments are *easy, efficient, and secure* to use[39].

7.1.1. Provisions applicable for implementing encryption

The most relevant provision within the PSD that could serve as the foundation of the use of encryption to protect the payment data is obligation

[36] European Commission, 2013: 7.
[37] http://ec.europa.eu/finance/payments/framework/index_en.htm.
[38] Payment System Directive, *What It Means for Consumers*.
[39] The EU Commission *press release* IP/07/1914, 12 December 2007.

of payment service providers to make sure that the personalised security features of the payment instrument are not accessible to other parties (Article 57)[40]. The key rule of this regulation is that for payment service providers it is an obligation to protect the consumer data against unauthorized access. Under law, obligation has always come with a consequence If not fulfilled. In this case, the consequence is ruled under Article 60 (1) of the PSD, which is to provide refund immediately to the consumer the amount of the unauthorised payment. In addition, consumers may, under Article 60(2), also request a financial compensation, provided that the contract concluded between the parties enables consumers to do so.

Another relevant provision under the PSD relating to the use of encryption is Article 79[41]. This article rules that if necessary to safeguard the prevention and detection of payment fraud, Member States shall permit payment systems and payment service providers to process personal data[42].

As the role of encryption in payment systems is to protect the data against any frauds, there are two key rules under the PSD relating to the use of encryption. The first is that the law permits the industry to do so, when needed. It is not an obligation or encouragement, but permitted when necessary. Who will decide when it is necessary to employ a more advance security such as encryption to prevent fraud: payment service provider, consumer, or regulator? Each has different point of view and interest that will lead to different types of regulations. Unfortunately, the PSD does not say much about it. The second key rule is that the PSD leaves it to the national level to enforce such a rule. This way, the PSD may create a different level and depth of regulations among the member states.

7.1.2. Does the existing framework suffice?

Overall, the PSD lays an implicit basic ruling regarding the obligation for payment service providers to implement encryption. This ruling, in form of obligation to take measures protecting the sensitive data, does not suffice to force the industry to implement specific measures such as end-to-end encryption in order to protect the data and prevent any breaches to occur

[40] There is another obligation imposed to payment service providers, which is to provide evidence relating to payment transactions. However, this obligation has less thing to do with the use of encryption, and therefore not discussed here.

[41] Chapter 4 of the PSD on Data Protection.

[42] The processing of data must be in accordance with Directive 95/46/EC on Data Protection.

again. The reason for laying down general ruling is that such ruling emphasizes on the technological neutrality and prevents the rules for being obsolete too fast, especially when a more advance security technology is invented. This actually is not a bad ruling. If accompanied by a more explicit and precise implementing regulation or a standard or code conduct agreed by the industry, this ruling could be an excellent one. However, there is no such clear cut implementing regulations requiring the industry to employ stronger measures to protect consumer data. In addition, industry standard has also loopholes. For card payments for instance, although encryption is encouraged by PCI DSS standard, it only emphasizes on the use of encryption for data in transit within public network, and slightly forgets data in transit within private network. What happened in major breaches such as that of Heartland Payment System is that the hacker stole consumer data while it was being transmitted within Heartland private networks. Hence, in order to protect consumer data at a better level, employing end-to-end encryption is crucial.

Another problem deals with the remedy available for consumer when an authorized transaction occurs. The PSD provides a weak ruling dealing with remedy for consumers for unauthorized transactions that had been made following a data breach at the service providers or third party processors. On the one hand, the PSD provides a general provision that the payment service providers must immediately refund to the consumer the amount of unauthorized transaction (under Article 60(1)). Although theoretically strong, this rule is lacking in power in practical. Consumers will find it difficult seeking redress as the providers will keep telling that by their system the unauthorized transactions have been "authorized" by consumers themselves. The fact is that the hackers have stolen the sensitive data needed for authentication and authorization, so the system will recognize the unauthorized payment order as authorized one. This loophole will always put consumers in a weak position.

On the other hand, the liability framework available for consumers, as provided mainly under Article 56 of the PSD, only applies to unauthorized transactions resulting from lost or stolen instruments. This is to say that this framework applies for "breach"[43] occurring from the consumer side (demand) while data & security breach occurs from the payment provider side (supply). Such framework includes zero liability for consumer after

[43] Fail to notify of any lost or stolen instruments, keep the instruments safe or involve in frauds or act gross negligence. See Article 56 of the PSD.

notification of any lost or stolen instruments, limited liability up to a maximum of EUR150 if consumer failed to keep the instruments safe, and full liability if consumer involved in fraud or acted gross negligence. As this liability framework focuses only on the demand side of online payments, it is not applicable to address liability for unauthorized transactions following a security/data breach (from supply side). Therefore, consumers of online payment systems suffering from security & data breaches will be left out unprotected.

7.1.3. Among the hype of innovative payments

Lacking of a strong ruling on security of online payment systems is worsened by the rise of new innovative payments. M-payments and virtual currencies, for instance, are types of innovative payments that often set-up by entities that are naturally familiar with security technology. In addition, alike that of many other retail payments, the ecosystem of m-payments and virtual currencies is rather sophisticated. In m-payments, in addition to the regular players of retail payments (such as service providers, retailers and consumers) the ecosystem also involves mobile device manufacturers and app developers and, often, telecommunication providers. While in virtual currencies, the ecosystem often includes start-up companies trying to enter the market for the first time, and in some cases such as in crypto- or peer-to-peer currencies involves crowd or community to authorize a transaction. This expanding ecosystem challenges the existing regulatory framework in the sense that it is difficult to apply the same framework over and over again to different systems.

The issue is even more complex when observing that the adoption of innovative payments is actually slow. One main issue hampering the adoption of m-payments is that the security employed in m-payments and the perceived security by consumers are low. As for the latter, for example, 38% of EU citizens do not trust in security of m-payments and therefore never willing use them.

There is a trade-off between security and accessibility of innovative payments. While a consumer will never use a system that he or she perceives unsecured, rigid security will possibly hamper the accessibility of the payment method as it will be less practical in terms of high cost and less convenience. This circumstance has given rise to regulatory challenges even more, as to how and to what extent authority should regulate m-payments that keep the balance between security and accessibility.

7.2. Proposal of Payment System Directive 2 (PSD 2)

In July 2013, the EU Commission published the Proposal of PSD 2. This new directive is expected to be officially issued and fully implement by 2016[44]. In such a draft, new players are brought in under the regulatory framework, aiming to encourage a variety of new low cost payment systems including m-payments by providing them with an appropriate regulatory framework[45]. This is to include the so-called third party payment service providers (TPPs), any party providing "*online banking base payment service*"[46] that currently does not fall under scope of existing regulatory framework. As a consequence, security requirements for payment instruments are strengthened, to include obligations covering operational, security and authentication (under Article 85). Under this proposed regulation, requirement to employ strong authentication is explicitly mention.

7.3. Other Regulatory Frameworks

Regulatory frameworks under the PSD and other laws on data protection and privacy and electronic communication regarding the use of encryption are alike. There is no strong provision to oblige industry to implement encryption, although this issue is slightly addressed in the proposed law on network and information security introduced in early 2013.

7.3.1. Data Protection Directive

The EU Directive on Data Protection was set in 1995, aiming at providing regulatory framework for data protection in the EU. It applies to so-called data controllers, the firms which responsible in determining the purpose (why) and means (how) of the processing of personal data[47]. Under Article 17 of the directive, Member States are required to implement "appropriate technical and organizational measures" in order to protect personal data against unauthorized disclosure. The directive, furthermore, rules that Member States shall also make sure that such measures enable to

[44] Proposal for PSD 2 (COM (2013) 547 final).
[45] Proposal for PSD 2 (COM (2013) 547 final): 2.
[46] See Impact Assessment in the Proposal for PSD 2 (COM (2013) 547 final): 6-7.
[47] See for instance Sotto et al., 2010.

maintain the security level to cope with the risk embedded by the processing of personal data as well as the nature of the data.

7.3.2. Privacy and Electronic Communication Directive

Although the Directive on Privacy and Electronic Communication basically applies to the electronic communication sector, some rules may also apply to the participants of online payment systems such as of m-payments because some m-payment providers also serve as telecommunication providers. Regulation relating to data security under this directive includes obligation of service providers to make sure that "*personal data can be accessed only by authorised personnel for legally authorised purposes*". In relation to encryption, there also lays general obligation that service providers must, at their best endeavour, protect data at rest and data in transit against various accidents including unauthorized or unlawful access or disclosure. However, under this legal framework there is no strong consequence affecting companies having consumer data breaches. The only consequence is that, under the EU Regulation 611/2013 on *the measures applicable to the notification of personal data breaches*, which took into effect by 25 August 2013, service providers suffering from data breaches must notify without undue delay any individuals affected by such breaches.

Even more, this obligation to notify can be set aside by service providers if they can prove that appropriate technology has been employed to "render the data unintelligible" to other party. Thus, under Regulation 611/2013 there is a safe harbour for service providers that implement appropriate encryption technology, which is not to notify their consumers affected by personal data breaches, provided that such encryption is able to maintain the data "unintelligible" to third party and the key of the encryption has not been compromised.

7.3.3. Law on encryption

"Law on encryption *per se* applicable within the EU is basically not in existence. However, the discussion on this issue can be dated back in 1990s, when the governmental bodies of some member states such as UK, the Netherlands, France and Spain investigated the misuse of encryption against state interests[48]. The discussion was mostly about restriction for export-

[48] Koops, 1996 and Koops, 1997.

import of encryption technology, and how to accommodate the state interest when an encryption technology is used by private entities. There were some suggestions to introduce a restriction on the use of encryption by private entities, by law. Although to certain extent this issue is still valid today, the main focus has actually shifted from "to restrict or not to restrict" to how to regulate the usage in proper manners, such as to protect consumer sensitive data and privacy.

8. CONCLUSION

Security breaches in online payment systems have often a significant financial outcome to not only payment providers but also consumers. Reviewing from the design of online payment systems, there is a weakest link within such online systems that leaves the system vulnerable to hacking. This vulnerability concerns the data in transit within private network are not protected. Some fatal data breaches, such as that occurring to Heartland Payment System in the US, stole consumer personal data while it was being processed within corporate payment network by installing malware enabling capturing the payment data. Hence, there is an emerging need for the industry to implement end-to-end encryption to protect not only data at rest but also data in transit within the public and private networks.

However, implementing end-to-end encryption to online payment systems is not an easy task. Online payment industry seems to be reluctant because of three main reasons. Firstly, economic reason, as implementing such security technology is not cheap. Costs incurred include budget for software implementation and hardware upgrades such as POS terminal and ATM, and not to mention human resource and time allocations. In another scenario where the starting point of end-to-end encryption is the payment instrument, the costs incurred include the cost for card replacement this not inexpensive. Secondly, obstacles coming from the design of online payment systems make the implementation of end-to-end encryption even more difficult. As such systems are created and used by private entities seeking mainly for profit, they become more precaution in calculating investment for security technology and in pricing. In addition, consumer perception of security in online payment systems plays a crucial role. If consumers perceived security as sufficient, such system will be widely accepted and used. These two factors may lead to payment providers ceased to improve the existing security.

The last reason is the obstacle arisen by the nature and characteristics of retail payment systems. As part of retail systems, online payment systems share the same nature and characteristics as those of retail systems. Two notable natures are, first, it involves small monetary value transactions, and, second, its ecosystem consists many parties. While the earlier makes the service providers more meticulous on IT investment, the later leads to coordination problems among the participants and interoperability issues among different systems.

Surprisingly, the existing laws and regulatory frameworks applicable within the EU provide basic rules to support the implementation of end-to-end encryption in online payment systems. Such laws and regulatory frameworks include law on payment systems, on data protection, on privacy and electronic communications, and on encryption. However, there are three flaws when it comes to the enforcement of the rules. Firstly, the frameworks do not explicitly mention the importance of encryption, rather than the obligation to employ "appropriate and adequate measures" to protect the personal data. This type of regulation is not necessarily a bad ruling. In fact, it could be an excellent regulation as long as followed by implementing regulation or guideline, or even a standard agreed by the industry. However, the latters have not yet in present. Secondly, the consequence for the payment service providers when they fail to fulfil the obligation has not adequate. The only explicit consequence is that such payment service providers are obliged to notify the affected individuals of any breach, with a safe harbour applicable for those that have already implemented appropriate measures to protect the personal data. Although this exemption could serve as an incentive for the industry to implement end-to-end encryption, merely rely on this incentive is not sufficient. Laws and regulatory frameworks need to explicitly mention such obligation that is followed by consequences with deterrent effect such as penalty. Otherwise, there is no strong will from the industry to improve the security of the systems. If this is the case, at the end the consumers will always the ones becoming the victims, especially in the hype of innovative payments where low security technology often employed.

Lastly, the redress and liability framework for a consumer set-up by the existing regulation is not adequate to address losses from data & security breaches that occur at the service providers (supply side of payment systems). The existing framework is too focus on financial losses from "breach" that occurs on the consumer side (demand side of payment systems) such as payment instruments being lost and stolen. This framework covers zero liability after consumer notifies his or her provider regarding lost and stolen instruments, limited liability if consumer fails to keep the

instruments safe and full liability if consumer involves in frauds or acts gross negligence. Although in the proposed regulation the limited liability for consumer is proposed to reduce from a maximum of EUR150 to EUR50, the liability framework for losses from breaches on the supply side has not been explicitly addressed. Therefore, in order to protect decent consumers of online payment systems, especially nowadays when many new innovative payments with expanding ecosystem and complicated back-end arrangement are available in the market, the existing redress and liability framework needs to be expanded to cover remedy for consumers suffering from data & security breaches.

References

- AL-MA'AITAH, M., and A. SHATAT. "Empirical study in the security of electronic payment systems." *IJCSI International Journal of Computer Science Issues* 8, no. 4 (2011).
- ANDERSEN, MADS BRYDE, and PETER LANDROCK. "Encryption and interception." *Computer Law & Security Review: The International Journal of Technology Law and Practice* 6, no. 12 (1996): 342-348.
- BISHOP, MATT. *Introduction to computer security*. Boston, MA: Addison-Wesley, 2005.
- BOLT, WILKO. "Retail Payment Systems: Competition, Innovation, and Implications." (2012).
- BOND, MIKE, OMAR CHOUDARY, STEVEN J. MURDOCH, SERGEI SKOROBOGATOV, and RICHARD ANDERSON. "Chip and Skim: cloning EMV cards with the pre-play attack." In *Security and Privacy (SP), 2014 IEEE Symposium on*, pp. 49-64. IEEE, 2014.
- BORESTAM, ANN, and HEIKO SCHMIEDEL. "Interchange fees in card payments." ECB Occasional paper 131 (2011).
- BOVELANDER, ERNST. "Smart Card Security 'How Can We Be So Sure?'." In *State of the Art in Applied Cryptography*, pp. 332-337. Springer Berlin Heidelberg, 1998.
- CAMENISCH, JAN L., JEAN-MARC PIVETEAU, and MARKUS A. STADLER. "Security in Electronic Payment Systems." Institute for Theoretical Computer Science, ETH Zurich. In: *Proceedings of the ESO RISKS* 94 (1994).
- CHENEY, JULIA S. "Heartland Payment Systems: lessons learned from a data breach." *FRB of Philadelphia-Payment Cards Center Discussion Paper* 10-1 (2010).
- DE SCHUTTER, BART. "Trends in the fight against computer-related delinquency." In *State of the Art in Applied Cryptography*, pp. 1-17. Springer Berlin Heidelberg, 1998.
- DESIMONE, TOM, Do You Really Need an EMV Chip Card Terminal?, Merchant Maverick, 24 September 2015, available at http://www.merchantmaverick.com/really-need-emv-chip-card-terminal/.
- EMVCO, *EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management*, Version 4.3, November 2011, available at https://www.emvco.com/specifications.aspx?id=223.
- EMVCO, *Worldwide EMV Chip Card Deployment* (online), available at http://www.emvco.com/about_emvco.aspx?id=202.
- EUROPEAN CENTRAL BANK, *Virtual Currency Scheme*, 2012.
- EUROPEAN COMMISSION, Directorate-General for Research and Innovation, Final Report from the Expert Group on Retail Sector Innovation, 30 October 2013, available at http://ec.europa.eu/research/innovation-union/pdf/Report_from_EG_on_Retail_Sector_Innovation_A4_FINAL_2.pdf.
- FREEH, LOUIS J. "Impact of encryption on law enforcement and public safety." *Trends in Organized Crime* 3, no. 1 (1997): 91-95.
- GJOMEMO, RIGEL, HAFIZ MALIK, NILESH SUMB, V. N. VENKATAKRISHNAN, and RASHID ANSARI. "Digital Check Forgery Attacks on Client Check Truncation Systems." In *Financial Cryptography and Data Security*, pp. 3-20. Springer Berlin Heidelberg, 2014.
- GOORDEN, SEBASTIANUS A., MARCEL HORSTMANN, ALLARD P. MOSK, BORIS ŠKORIĆ, and PEPIJN WH PINKSE. "Quantum-secure authentication of a physical unclonable key." *Optica* 1, no. 6 (2014): 421-424.
- GORDON, LAWRENCE A., MARTIN P. LOEB, WILLIAM LUCYSHYN, and ROBERT RICHARDSON. "2005 CSI/FBI computer crime and security survey." (2005).

- HUGHES, BARRY, DAVID BOHL, MOHAMMOD IRFAN, ELI MARGOLESE-MALIN, and JOSÉ SOLÓRZANO. "Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance." *Frederick S. Pardee Center for International Futures* (2015).
- IT POLICY COMPLIANCE GROUP. "Core Competencies for Protecting Sensitive Data". *Benchmark Research Report*, October 2007.
- JOHNSON, OMOTUNDE EG. *Payment Systems, Monetary Policy and the Role of the Central Bank*. International monetary fund, 1998.
- KHIAONARONG, TANAI, and JONATHAN LIEBENA. *Banking on innovation: modernization of payment systems*. Springer Science & Business Media, 2009.
- KIM, CHANGSU, WANG TAO, NAMCHUL SHIN, and KI-SOO KIM. "An empirical study of customers' perceptions of security and trust in e-payment systems." *Electronic Commerce Research and Applications* 9, no. 1 (2010): 84-95.
- KOOPS, BERT-JAAP. "A survey of cryptography laws and regulations." *Computer Law and Security Report* 12, no. 6 (1996): 349-355.
- KOOPS, B-J. "Crypto regulation in Europe. Some key trends and issues." *Computer networks and ISDN systems* 29, no. 15 (1997): 1823-1831.
- LAUDON, KENNETH C., and CAROL GUERCIO TRAVER. *E-commerce*. Pearson/Addison Wesley, 2007.
- LEWIS, DAVE. "Heartland Payment Systems Suffers Data Breach". Forbes, 31 May 2015. Available at http://www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach/.
- MOORE, TYLER, and RICHARD CLAYTON. "The Ghosts of Banking Past: Empirical Analysis of Closed Bank Websites." In *Financial Cryptography and Data Security*, pp. 33-48. Springer Berlin Heidelberg, 2014.
- MURDOCH, STEVEN J., SAAR DRIMER, ROSS ANDERSON, and MIKE BOND. "Chip and PIN is Broken." In *Security and Privacy (SP), 2010 IEEE Symposium on*, pp. 433-446. IEEE, 2010.
- MURDOCH, STEVEN J., and ROSS ANDERSON. "Security protocols and evidence: Where many payment systems fail." In *Financial Cryptography and Data Security*, pp. 21-32. Springer Berlin Heidelberg, 2014.
- ONDRUS, JAN, and YVES PIGNEUR. "Near field communication: an assessment for future payment systems." *Information Systems and E-Business Management* 7, no. 3 (2009): 347-361.
- Payments Leader, Will retailers be ready for EMV by Oct 2015?, available at http://www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015/.
- Payment System Directive, *What It Means for Consumers*, available at http://ec.europa.eu/internal_market/payments/docs/framework/psd_consumers/psd_en.pdf.
- Payment System Directive: Commission encourages swift and coherent implementation at national level, *press release IP/07/1914*, 12 December 2007, http://europa.eu/rapid/press-release_IP-07-1914_en.htm?locale=en.
- PERL, HENNING, SASCHA FAHL, and MATTHEW SMITH. "You Won't Be Needing These Any More: On Removing Unused Certificates From Trust Stores." In *Financial Cryptography and Data Security*, pp. 307-315. Springer Berlin Heidelberg, 2014.
- PRENEEL, BART. "Cryptographic primitives for information authentication—State of the art." In *State of the Art in Applied Cryptography*, pp. 49-104. Springer Berlin Heidelberg, 1998.

- PRENEEL, BART, VINCENT RIJMEN, and ANTOON BOSSELAERS. "Recent developments in the design of conventional cryptographic algorithms." In *State of the Art in Applied Cryptography*, pp. 105-130. Springer Berlin Heidelberg, 1998.
- RANKL, WOLFGANG, and WOLFGANG EFFING. *Smart card handbook*. John Wiley & Sons, 2010.
- RODE, LILIA. "Database security breach notification statutes: does placing the responsibility on the true victim increase data security." Hous. L. Rev. 43 (2006): 1597.
- SCHMIEDEL, HEIKO, GERGANA L. KOSTOVA, and WIEBE RUTTENBERG. "The social and private costs of retail payment instruments: a European perspective." ECB Occasional paper 137 (2012).
- SCHMALENSEE, RICHARD, and DAVID S. EVANS. "The economics of interchange fees and their regulation: An overview." (2005).
- SCHOENMAKERS, BERRY. "Basic security of the e-cash payment system." Computer Security and Industrial Cryptography: State of the Art and Evolution, LNCS series (1997).
- SOTTO, LISA J., BRIDGET C. TREACY, and MELINDA L. MCLELLAN. "Privacy and Data Security Risks in Cloud Computing." World Communications Regulation Report 5, no. 2 (2010): 38.
- SULLIVAN, RICHARD J. "Controlling security risk and fraud in payment systems." *Federal Reserve Bank of Kansas City, Economic Review* 99, no. 3 (2014): 47-78.
- TURBAN, EFRAIM, and JOSEPH BRAHM. "Smart card-based electronic card payment systems in the transportation industry." *Journal of Organizational Computing and Electronic Commerce* 10, no. 4 (2000): 281-293.
- VEDDER, KLAUS, and FRANZ WEIKMANN. "Smart cards—Requirements, properties, and applications." In *State of the Art in Applied Cryptography*, 307-331. Springer Berlin Heidelberg, 1998.
- YUNG, MOTI. "Cryptographic protocols: from the abstract to the practical to the actual." In *Financial Cryptography and Data Security*, 1-2. Springer Berlin Heidelberg, 2012.
- ZULHUNDA, SONNY, IDA MADIEHA, and ABDUL GHANI AZMI. "Security Safeguards on e-Payment Systems in Malaysia: Analysis on the Payment Systems Act 2003." *J. Int'l Com. L. & Tech*. 6 (2011).