Collaboration and the sharing of information help reduce payment transactions fraud

Marco Doeland

Received (in revised form): 3rd January, 2017

Dutch Payments Association, PO Box 83073, Amsterdam 1080AB, The Netherlands
Tel: +31 20 305 1971; E-mail: m.doeland@betaalvereniging.nl

Marco Doeland *is Head of Risk Management at the Dutch Payments Association. He is also Chairman of the Security Task Force at the Dutch National Forum on the Payment System (MOB) and Chairman of the Interbank Security Task Force. In addition, he is a member of the Financial Services — Information Services and Analysis Center (FI-ISAC) and the Interbank Business Continuity Forum.*

Abstract

In recent years, the Netherlands has benefited from the voluntary cooperation between various parties that play a role in the payment chain. For example, knowledge and experience in the field of fraud prevention and cyber security are shared and exchanged, more research and threat analyses are conducted, and fraud mitigation measures are coordinated and implemented jointly. This domestic partnership is unique in Europe. The Dutch Payments Association manages the collective aspects of cyber security policy in relation to the payment system, and works closely with other institutions, including the National Cyber Security Centre, to implement this policy. It also coordinates fraud prevention within the entire payment chain, compiles and analyses statistics on fraud, and drafts prevention policy. In addition, it coordinates the implementation of measures designed to prevent fraud. This unique Dutch partnership limits cyber crime and fraud. Any payment chain is only as strong as its weakest link, however; therefore, cooperation between the various parties involved is vital to ensure and enhance security in the payment chain. This paper describes the Dutch approach to fighting fraud in the payment system.

Keywords: cyber security, cyber crime, electronic payments, Netherlands, Europe, fraud figures

INTRODUCTION

In recent years, fraud that involves online banking and payment cards has declined significantly in The Netherlands, partly because those parties who have an important part to play in the world of payment transactions collaborate closely when it comes to fraud detection and prevention. This decline has also been noticed in the rest of Europe. What has The Netherlands been doing to achieve this, and what can other sectors and countries learn from this?

THE ROLE OF THE DUTCH PAYMENTS ASSOCIATION

The Dutch Payments Association (DPA) seeks to achieve a socially efficient, secure and reliable payment transactions system. Risk management plays an important role in this regard, as the payments system has to be both efficient and secure. On behalf of its members, the DPA organises tasks for the national payments system. Its members are providers of payment services: banks, payment institutions and electronic money institutions. The DPA works on such tasks as standards for the payment transactions infrastructure and shared product features. This includes standards for the clearing and settlement of card transactions and

Marco Doeland

Journal of Payments Strategy & Systems
Vol. 11, No. 1 2017, pp. 81–85

payments made through iDEAL (the Dutch e-commerce payment platform that enables consumers to make online payments through their own bank),[1] as an efficient payments system would be impossible if banks were to use different standards. However, the Dutch payments system is in fact very efficient, thanks in part to well thought-out arrangements between the parties involved.

The Dutch economy is highly dependent on having a payments system that works well. Private individuals, retailers, companies and financial institutions must be confident that card payments, payment transfers and other payment transactions will be carried out quickly and correctly at all times. This means there must be a good, active collaboration between the providers of these payment services and the representatives of end users, including consumers and entrepreneurs. The DPA brings all these parties together.

The public interest in having an efficient and secure electronic payment system in The Netherlands has increased significantly in recent years. As a result, the value of online, card and mobile payments has increased from €2,800bn in 2012 to €3,500bn in 2015.[2] These developments have also increased the need to make payments more secure, to combat fraud more stringently, and to prevent disruptions at an earlier stage.

FRAUD AND UNAVAILABILITY

Technical faults in the payment chain can prove a hindrance to consumers and entrepreneurs alike, which in turn leads to dissatisfaction and complaints. Unavailability, caused for instance by a distributed denial of service (DDoS) attack, can have a major impact on the provision of banking and payment services. In addition, there are whole host of fraud types, including online banking fraud like phishing and malware, and various types of card fraud, such as skimming, theft and cash trapping.

Many different parties have important roles to play in the combating of fraud, including banks, transaction processors, suppliers of point-of-sale (POS) terminals and card scheme owners (MasterCard, Visa), not forgetting entrepreneurs or consumers. Police forces and law enforcement agencies have a major role to play in tracking down fraudulent criminals. Preventing and combating fraud is something that requires teamwork.

The DPA coordinates and facilitates the implementation of measures that aim to achieve a secure and reliable payments system. Furthermore, it monitors the security and reliability of the electronic payments system and analyses incidents, threats and risks, and also supervises fraud prevention activities. It also encourages new developments that help to make the payments system safer, more secure and affordable for all stakeholders, both now and in the future. The introduction of contactless card payments, mobile banking, and the further development and implementation of quick response codes for the Dutch online payments system known as iDEAL are some important examples. Finally, the DPA is currently developing, in close collaboration with its members, a new infrastructure for real-time payments (Instant Payments).

SKIMMING AND ONLINE BANKING

To prevent skimming of the magnetic strips on the back of payment cards, by the end of 2011 all Dutch payment cards were replaced by new cards with a chip that is better protected than the magnetic stripe. Furthermore, POS terminals and cash dispensers (ATMs) were modified in order to use this chip when card payments and withdrawals are made. Nevertheless, these measures, which followed the implementation of the Single Euro Payments Area (SEPA) Cards Framework requirements, did not stop skimming. To prevent fraudulent transactions

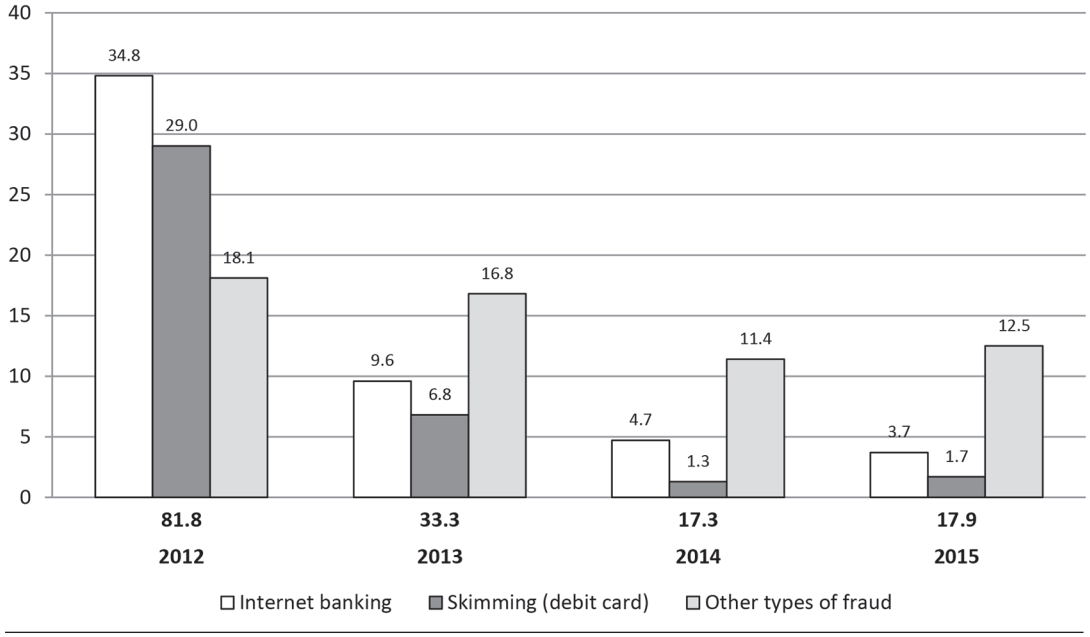

Figure 1 Losses due to fraud in the payment system, 2012–2015 (€m/year)

taking place outside of European borders, all major Dutch banks implemented geo-blocking, thereby preventing Dutch debit cards from being used outside Europe for cash withdrawals or POS transactions unless previously unlocked by their owners. As a result, it is no longer profitable for criminals to skim a Dutch payment card. Up to mid-2013 skimming of payment cards was always one of the two largest fraud losses; since 2014, however, skimming has become a relatively minor loss item.

Fraud targeting online banking has also been drastically reduced in recent years, as shown in Figure 1. The successful Dutch television and internet campaign 'Hang up, click away, phone your bank'[3] has had a major impact in this regard, as has the sharing of information about security incidents and criminals *modus operandi*, both within the banking system and with the authorities in public–private partnerships. In addition, transaction monitoring, which detects transactions that deviate from normal transactions, has also heavily contributed to the decline of online banking fraud. A further decline of the total fraud figure over 2016 is expected and will be published at the latest April 2017.

RESEARCH INTO THE DUTCH APPROACH, AND SIMILARITIES AND DIFFERENCES WITHIN EUROPE

Research[4] was conducted to scrutinise the main features of the Dutch approach to cyber security within the financial sector. In addition, the main features of the Dutch approach were compared with those of 13 European countries. Within Europe, The Netherlands is viewed as a leader in this field, particularly given the above-mentioned decline in electronic banking fraud over the past three years.

Other countries have experienced just the opposite, which means that a better understanding of the Dutch approach could be very useful for managers and employees who are involved in cyber security.

Following a two-step Delphi research method and with the help of the participants in the Dutch Financial Institutions

Information Sharing and Analysis Centre (FI-ISAC), a public–private partnership, the following top five characteristics of the Dutch model were identified:

- agreement that banks will not compete on security;
- information exchange between banks;
- collaboration between banks, to include the shared delivery of products and services;
- collaboration between banks and public and private sectors; and
- strong technical security measures.

The agreement that banks will not compete on security created the basis for both the sharing of information and for collaboration. The key features of the Dutch model have been identified as the exchanging of information between the payment services providers, and collaboration within the private sector (via the provision of shared products and services, including in respect of cyber crime and intelligence, and the joint awareness-raising 'Hang up, click away, phone your bank' campaign). The collaboration between the public and private sectors is another key feature, with the appointment of the first banking liaison officer in 2013. The liaison officer is appointed by the financial sector via the DPA, and his workplaces are the Dutch government ministries in The Hague and the collaborating banks. A final measure was the implementation of a number of technical measures such as stringent customer authentication and fraud detection. These are the aces deployed in the Dutch approach to cyber security within the financial sector.

SIMILARITIES AND DIFFERENCES WITHIN EUROPE

The second part of the research was the comparison of the five main features of the Dutch approach with those of 13 European countries. This comparison revealed a number of similarities and differences. The EU-ISAC country representatives of 13 European countries were interviewed using semi-structured interviews. The sharing of information, collaboration, and the gaining of trust are important issues when it comes to safeguarding security, with both public and private players. A number of similarities with the Dutch approach were found in the 13 researched European countries. These similarities are stringent technical security measures, information exchange between the banks themselves and the agreement that banks will not compete on security.

However, differences between the Dutch approach and that taken in the other countries were found in respect of collaboration too. Specifically, these relate to collaboration between the banks themselves and to the collaboration between the banks and the public and private sectors. No more than half the interviewed countries had the same type of collaboration as exists in The Netherlands. One measure taken in The Netherlands — but not yet implemented by some other European countries — is to intensify the sharing of information in order to improve collaboration further, for example, by creating joint cyber security intelligence sources that can be used by a range of stakeholders both within the sector and between the sector and the authorities. A second piece of research carried out as part of this thesis delivered results that confirmed these conclusions. Collaboration between the public and private sectors in Europe was perceived to be poorer than the collaboration within the private or public sector.

HINDERING FACTORS

The research also discovered two 'hindering factors' that prevent the progress from information-sharing to active collaboration. The country representatives named these factors as possible reasons why there are differences versus the Dutch approach. First of all, legislation can prove a hindrance, in particular the laws relating to privacy issues,

as they can hinder the sharing of information. Secondly, a number of countries view the anti-cartel legislation as a barrier to the active sharing of information and to actual or improved collaboration.

FURTHER COLLABORATION WITHIN EUROPE

The DPA will use the results of this research to maintain a secure, stable and robust payments system. The five main features of the Dutch model will continue to be embraced. In addition, The Netherlands is able to share the knowledge that it possesses on cyber security. This means that the level of security in other countries can be improved further, allowing the number of incidents of fraud to be reduced there too. It is important to involve and advise the parties concerned, to ensure that information is exchanged and that these parties collaborate, not just in The Netherlands but as well in the rest of Europe. The DPA is an active member of a number of Dutch and European steering committees and task forces in the field of payment transactions and security; the insights in and conclusions from this thesis will help to create a safer, more secure world for digital payments. In the end, it all boils down to collaboration and trust.

References and Notes

(1) In addition to webshops, other online organisations that are not part of the e-commerce market also offer iDEAL. iDEAL is increasingly used to pay energy bills, make donations to charities, buy mobile credits, pay local taxes, traffic fines, etc.

(2) Dutch Central Bank (2016) 'Payment statistics', available at: http://www.dnb.nl/en/statistics/statistics-dnb/financial-institutions/banks/payment-statistics/index.jsp (accessed 21st February, 2017).

(3) Dutch Payments Association (2016) 'Safe banking in the Netherlands', available at: https://www.veiligbankieren.nl/en/ (accessed 21st February, 2017).

(4) The research was conducted under a non-disclosure agreement. In-depth results of the research are therefore not publicly available. A summary of the research is available upon request.