How to keep payments safe and secure in a changing world

Marco Doeland

Received (in revised form): 27th March, 2019

Dutch Payments Association, PO Box 83073, Amsterdam 1080AB, The Netherlands
Tel: +31 20 305 1900; E-mail: m.doeland@betaalvereniging.nl

Marco Doeland

Marco Doeland *is Manager Risk Management at the Dutch Payments Association, where he is responsible for managing shared interests with respect to the (cyber) security of Dutch payment infrastructures, including online, cards, mobile, iDEAL (the Dutch e-commerce payment platform) and iDIN (the Dutch online identity scheme). He is also Chief Information Security Officer at Currence, Chairman of the Security Task Force at the Dutch National Forum on the Payment System, and Chairman of the Interbank Security Task Force. In addition, he is a member of the Dutch, European and Global Financial Institutions — Information Services and Analysis Centers.*

Abstract

In recent years, The Netherlands has benefited from voluntary cooperation between the various parties in the payment chain. For example, knowledge and experience in the field of fraud prevention and cyber security are shared, there has been an increase in the volume of research and threat analysis conducted, and fraud mitigation measures are now coordinated and implemented jointly. With the introduction of Instant Payments and the Revised Payments Services Directive, an increased focus on the availability of payment services and the feasibility of greater control regarding the prevention of authorised push payment fraud, Dutch banks have introduced various measures to keep electronic payments safe and secure in a rapidly changing world. This paper describes the latest developments in the world of payments, identity and security measures to reduce fraud without compromising availability or security.

Keywords: cyber security, cyber crime, instant payments, PSD2, Netherlands, online identity, iDIN

INTRODUCTION

In recent years, The Netherlands has enjoyed a significant decline in online banking and payment card fraud,[1] partly because those parties with an important part to play in the world of payment transactions collaborate closely when it comes to the prevention and detection of fraud.

Such partnership at the domestic level is unique in Europe. The Dutch Payments Association (DPA) 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 to prevent fraud. This unique partnership contains cyber crime and fraud in the payment chain. However, every chain is only as strong as its weakest link; for this reason, cooperation between the various parties involved is vital to ensure and improve security in the payment chain.

In 2019, two major changes on payments will be introduced in the Dutch market. The first is the introduction of Instant Payments and the second is the introduction

Journal of Payments Strategy & Systems
Vol. 13, No. 2 2019, pp. 132–137

of the Revised Payments Services Directive (PSD2). These changes will have a major impact on the payments system and introduce possible new threats and new forms of fraud. The Dutch banks have therefore agreed to continue their shared efforts to mitigate the risks and keep fraud at its current level. Recently, Dutch banks have taken extra measures to prevent their customers from executing fraudulent authorised push payments. In addition, the banks have introduced iDIN (https://www.idin.nl/en/), an online identity scheme to help their customers conduct their online activities safely.

THE ROLE OF THE DUTCH PAYMENTS ASSOCIATION

The DPA seeks to achieve an efficient, secure and reliable payment transaction system. Risk management plays an important role in this regard, as the payments system must be both secure and reliable. On behalf of its members, the DPA organises the shared tasks for the national payments system. Its members are providers of payment services: banks, payment institutions and electronic money institutions. The DPA is involved in topics such as standards for the payment transactions infrastructure and shared product features. This includes standards for the clearing and settlement of card transactions and payments made through iDEAL (the Dutch e-commerce payment platform that enables consumers to execute online payments through their own bank), as an efficient payments system would be impossible if banks were to use different standards. 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, money transfers and other payment transactions will be carried out quickly and correctly at all times. This means there must be a good and active collaboration between the providers of these payment services and the representatives of end users, including consumers and merchants. The DPA brings all these parties together.

Within The Netherlands, the need for an efficient and secure electronic payment system has increased significantly over the last few years, as demonstrated by the value of online and mobile payments increasing from €3.11bn in 2014 to €3.51bn in 2018.[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.

DUTCH BANKS ARE BECOMING IDENTITY PROVIDERS

Due to the rapid growth in digital services, businesses and institutions have an increasing need for certainty regarding the identity of online customers and users. Banks are offering their services based upon the trust they deliver. In 2017, the Dutch banks launched iDIN. With iDIN, consumers can identify and authenticate themselves easily, and can significantly reduce the number of (online) accounts they need because there is a smaller chance of forgetting a password. Further, consumers are assured of a secure login method, so they do not have to provide their data repeatedly. For merchants, this saves time, manpower and paperwork and increases conversion rates. In short, iDIN results in increased efficiency in online identification, with a focus on user convenience, return on investment and stricter security and privacy requirements imposed by legislation. The service comprises a variety of product types that can be used in different use cases, offering identification, login and age confirmation.

HELPING CUSTOMERS AVOID EXECUTING FRAUDULENT AUTHORISED PUSH PAYMENTS

Authorised push payment fraud is a form of fraud in which victims are deceived or manipulated into making payments under false pretences to a bank account controlled by a fraudster. An important example of this fraud category is the so-called invoice fraud. In such instances, the IBAN on an invoice is manipulated by the fraudster so that any money transferred goes directly to the fraudster's bank account. To mitigate this fraud and to give users more information about the beneficiary, Dutch banks introduced the IBAN Name Check service[3] — a unique service within the European Payments Council Single Euro Payments Area (SEPA) scheme.

This innovative — and free — internet and mobile banking service checks whether the name associated with the Dutch IBAN of the beneficiary matches with the name of the beneficiary entered by the customer before the credit transfer is executed. The simple process helps the customers of Dutch banks protect themselves against account number fraud and hence avoid incorrect transfers. When an internet or mobile banking user has entered the IBAN and name of the beneficiary, the name is checked before the transfer is executed. If the check reveals any errors, the user will receive a warning, and if the error is marginal, the correct name of the beneficiary bank account is suggested.

It is worth mentioning, of course, that under European legislation, the IBAN is the unique identifier used for routing transactions; in other words, the beneficiary name is not strictly relevant for the actual transfer. For this reason, customers remain responsible for how they respond to the warning.

BANNING TECH SUPPORT SCAMS

A second example of authorised push payment fraud leading to frustration and reduced trust in electronic payments is the tech support scam. Such scams comprise several types of fraudulent activities in which a fraudster telephones their potential victim and claims to offer legitimate technical support services. These telephone calls take the form of 'cold calling' unsuspecting users, or inducing users to call a certain telephone number, for instance via a browser pop-up. In The Netherlands these scams are primarily aimed at Microsoft or Apple users, with the caller often claiming to represent the technical support services of these companies.

The fraudster will typically try to induce the victim to allow him or her remote access to the victim's computer. After remote access has been obtained, the fraudster will try to win the victim's trust by providing so-called 'support'. Subsequently, the victim will be induced to transfer money to the fraudster via a bank or money transfer, or the victim will be tricked in some other way to pay up.

In 2017, the various tech support scams in The Netherlands resulted in almost 1,900 registered police reports and almost €6m in losses. To combat the problem, various parties, including government, tech platforms, telecommunication providers, international money transfer companies, Dutch banks, Dutch Payments Association and the United Bitcoin Companies formed a broad coalition.

These parties are aiming to prevent tech support scams in their current form in The Netherlands before the end of 2020. Awareness, monitoring and technical measures are key pillars in achieving this result.

AVAILABILITY AND DDOS ATTACKS

Given the increased use of online banking and electronic payments, the availability of such services is more important than ever. Since 2017, The Netherlands has enacted legislation ensure the availability of the Dutch

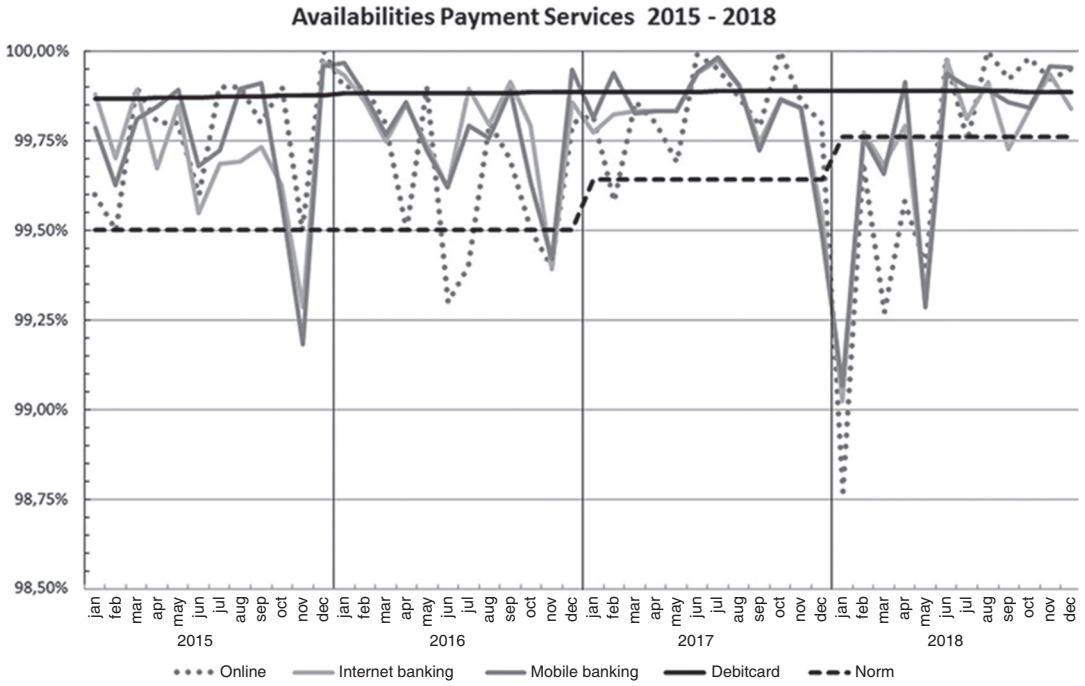

Figure 1: Availability of Dutch banks online/ electronic banking and payments services (percentage up-time/ year), 2015–2018

iDEAL e-commerce payments scheme and point-of-sale card transactions (both debit and credit).[4] Such legislation, to the author's knowledge, is unique to The Netherlands. The legislation started in 2017 and guaranteed a minimum availability or up-time of 99.64 per cent. This was increased to 99.76 per cent for 2018, and in 2019 it reached its final level of 99.88 per cent.

The DPA publishes figures regarding the service availability of its members on its website, enabling transparency and trust. If a bank fails to deliver on the mandatory availability percentage, it must provide a written explanation to the Dutch Central Bank. Figure 1 shows the availability of the Dutch banks for online/electronic banking and payments services.

In January 2018, several banks and other service providers suffered heavily from distributed denial of service (DDoS) attacks on their websites and online services. To mitigate the impact of DDoS attacks, Dutch banks have taken a number of measures, the specifics of which have all been shared with the Dutch banking and payments community.

DDoS attacks come in two basic forms: attacks on bandwidth volume and attacks using malicious applications. Dealing with the latter is especially difficult, and demands considered decision-making between mitigation partners. The DPA has also made it straightforward for its members to report DDoS attacks so that the police and prosecutor can act. As a result, several booter and stresser websites used to carry out DDoS attacks have been dismantled and the perpetrators arrested.[5] The banks have enhanced their mitigation measures and a public–private partnership has been established to tackle future attacks.

THE DUTCH INSTANT PAYMENTS SEPA CREDIT TRANSFER

Real-time transfers between accounts held at the same Dutch bank (so called *on-us*

transactions) have been possible for a couple of years now. In addition, since November 2017, ABN AMRO has offered instant payment transactions with a number of European banks. Following the adoption of instant payments by the Dutch banks in early 2019, this real-time experience will soon become the new normal for transfers between accounts held at different Dutch banks. With Dutch instant payment credit transfers, funds are available for the recipient to use within five seconds, 24/7. This service is based on the European standard, making transactions between Dutch and European banks possible. The Dutch service, however, includes two important extras: a maximum time to process of five seconds and the absence of a maximum amount.

The Dutch banking community believes that instant payment transaction volumes will increase quickly, making instant payments the *de facto* standard for payments. Instant payments are also interesting from the perspective of the fraudster, as money obtained fraudulently can be transferred instantly, giving banks no time to investigate the transaction manually, if necessary. The Dutch instant payments scheme, however, contains an extra measure to provide information on the trustworthiness of the transaction. This data record can be used for further enquiries by the beneficiary bank. Furthermore, if the transaction is considered fraudulent, the originating bank will not submit the transaction at all. In the event of doubt, the originating bank can use this extra measurement to inform the beneficiary bank. The beneficiary bank can then use this information, with its own knowledge about the beneficiary customer, to decide what to do with the transaction. In addition, as soon as the received payment leads to a new payment, a more complete analysis (debit detection) can be made. With this measure, the Dutch banks believe that fraud within the Dutch instant payments scheme will be severely curtailed.

PSD2, THE DUTCH NATIONAL IMPLEMENTATION SUPPORT PLATFORM

The PSD2 has a significant impact on the banking and payments landscape. Under PSD2, banks — known as account servicing payments service providers (ASPSPs) — are obliged to offer a digital gateway to regulated third-party providers (TPPs) that can initiate payments and/or provide account information services. Obtaining access is possible via the consumer interface or a dedicated application programming interface (API). The DPA supports the view that open, specially developed dedicated interfaces or APIs provide the best guarantee for safe and reliable communication via the banking infrastructure between third parties and payment account holders. Individual payment service providers and European market standardisation initiatives support this direction and the DPA is closely involved.

Under PSD2, ASPSPs might lose some of the information they currently use within their transaction monitoring. As with any change, the PSD2 introduces new opportunities and challenges for banks. For example, to monitor transactions, banks must obtain data they no longer possess, including biometric and behavioural data or details about the customer's mobile device. Under PSD2, only the provision of the IP address is mandatory; however, the use of other data fields is preferential for security reasons and transaction monitoring. Within PSD2, three strong customer authentication (SCA) options are possible: redirect, decoupled and embedded. An ASPSP can choose which SCA option they offer to the TPPs.

The DPA is undertaking coordination activities to facilitate the implementation of dedicated interfaces for both ASPSPs and TPPs. These activities are taking the form of the 'National Implementation Support Platform NL' (https://www.betaalvereniging.nl/en/focus/nisp-nl/). This platform facilitates the interaction between ASPSPs, TPPs and

other stakeholders, with the Dutch Central Bank as an observer. With this approach, the DPA aims to facilitate the smooth implementation of PSD2 within The Netherlands.

EXPANDING THE DUTCH APPROACH WITHIN EUROPE AND THE REST OF THE WORLD

The DPA will use its relations and various roles to maintain a secure, stable and robust payments system. The experience of The Netherlands illustrates that cooperation can lead to a more safe and secure payments world. 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 in the rest of Europe, too. 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, including the European Banking Federation, European Payments Council, and the European and Global Financial Institutions — Information Services and Analysis Centers. The DPA is also responsible for chairing the European Card Payments Association Security Working Group, and as such enjoys membership of the PCI Security Standards Council Board of Advisors.[6]

References

(1) Doeland, M.M. (2017) 'Collaboration and the sharing of information help reduce payment transactions fraud', *Journal of Payments Strategy & Systems*, Vol. 11, No. 3, pp. 81–85.

(2) Dutch Payments Association (2018) 'Facts and figures on the Dutch payments system in 2018', available at https://factsheet.betaalvereniging.nl/en/ (accessed 25th April, 2019)

(3) Dutch Payments Association (2017) 'Dutch banks introduce innovative IBAN-Name Check', press release, available at https://www.betaalvereniging.nl/en/actueel/persberichten/dutch-banks-introduce-innovative-iban-name-check/ (accessed 26th March, 2019).

(4) Dutch Government (2015) 'Regeling van de Nederlandsche Bank N.V. van 8 December 2015 ter uitvoering van artikel 26b van het Besluit prudentiële regels Wft (Regeling Oversight goede werking betalingsverkeer)', available at: https://zoek.officielebekendmakingen.nl/stcrt-2015-46628.html (accessed 26th March, 2019).

(5) Dutch National Police Corps (2018) 'Operation Power Off — Police close down largest DDoS website', available at https://www.politie.nl/nieuws/2018/april/25/operation-power-off-%E2%80%93-police-close-down-largest-ddos-website.html (accessed 26th March, 2019).

(6) European Card Payment Association (2019) 'PCI SSC Board of Advisors', press release, available at: https://www.europeancardpaymentassociation.com/wp-content/uploads/2019/02/2019-2020-PCI-SSC-Board-Members-Announcement.pdf (accessed 26th March, 2019).