Fighting CNP fraud - a Case Study

Marc Sel

PwC

marc.sel@pwc.be

Abstract

This article discusses fraud and fraud fighting techniques, particularly in an Internet-based CNP (Card Not Present) context. This scenario continues to be increasingly popular. We will illustrate it with a case study for an airline. As non-cash payments increase with our mobile life-style, so does the use of credit card payments over the Internet. Such use is referred to as CNP (Card Not Present), since the Merchant accepting the card has no contact with the card-holder except for the electronic transaction that is carried out. As there are many parties involved (merchant, service provider for IT services and website, payment providers, acquiring and issuing banks, switch, etc), determining liability in case of fraud is often not trivial. We will describe a real-world case, where the merchant experienced a fraud rate of more than 4% on his Internet payments. We will discuss the technical and legal safeguards that were implemented to fight the various frauds that were taking place. These safeguards concentrated on the implementation of 3D Secure for the CNP transactions, legal action, and an improvement of logical access controls for the airline reservation platform.

1 Context

Fraud and fraud-fighting will most likely continue to go hand-in-hand. In the context of our client, Airline Z999 (real name withheld), fraud had gradually been ramping up over some years to reach an unacceptable level.

There were two major components of the fraud. One component consisted of what could be referred to as "value chain" fraud, where employees engaged in fraudulent transactions such as selling tickets for a high price, delivering lower value tickets and pocketing the difference. Most of this fraud was addressed though improvement of logical access controls and complementary safeguards. This is not addressed here.

The other component consisted of "CNP (Card Not Present)" fraud with credit card sales over the internet. This is addressed further in this article. As the statistics of e.g. the European Central Bank and Eurostat show, card payments are increasing and will most likely continue to increase. For this reason, many different and complementary initiatives have been undertaken to fight card fraud. Credit cards are issued by an entity such as a bank. The issuer may outsource some of the activities to a service bureau. Issuance is governed by a scheme (e.g. VISA or MasterCard for credit cards). Regulation known as KYC (Know Your Customer) was enforced to make sure banks are reasonably sure who they serve or issue credit cards to.

Obvious, while significant attention has been paid to establishing and operating schemes, this should be seen in the light of the basic challenges that apply to identity management. This includes approaches that diverge widely across the globe with regard to issuing identity cards.

However such cards are used as a bootstrap security measure by the issuers. While in Europe, the European Commission in the context of the Digital Agenda announced plans to issue an eAuthentication directive, it is clear that the practical consequences of it are still a long way ahead.

Equally important are the different implementation speeds with regard to EMV's "pin & chip" [EMVCO], leaving a window of opportunity for fraudsters that deploy skimming techniques (copying the magstripe information of a credit card, which may be combined with capturing the PIN e.g. using a tiny camera).

Furthermore for many years we witnessed the roll-out of the guidelines of the Payment Cards Industry forum [PCIDSS]. Their "Data Security Standard" aims at the protection of cardholder data, used in transaction, settlement, reconciliation, chargeback, loyalty rewards, marketing, etc. A company acting in payment transactions is expected to comply with these guidelines. An important technique is the limitation of the Cardholder Data Environment (CDE), where it is suggested to use the credit card in transaction, but once authorised, sent the cardholder data to a "secure vault" and replace it either by an encrypted version, or a random unique number ("tokenization"). However, bear in mind that the PCI guidelines mainly protect the others from potential mistakes that you as a merchant could make, not the other way around. That such measures make sense has been demonstrated for example by the well-known Hannaford case in the United States, where data of approximately 4.2 million cards was stolen in 2008.

-

2 Problem and analysis

2.1 A short description of the problem

Airline Z999 was experiencing a cumulated 4,5+% fraud on ticket sales with regard to one particular African country. The main reason for this was a high amount of "chargebacks", i.e. cases where the cardholder denies having placed the order and requesting to reverse the transaction. The set-up was such that no liability was taken by any party in the chain such as issuer, processor, acquirer, etc. As a consequence the merchant (Airline Z999) was taking the losses. When cardholders claimed they did not authorise a particular transaction, they were refunded at the merchant's expense.

The overall set-up can be depicted as follows:

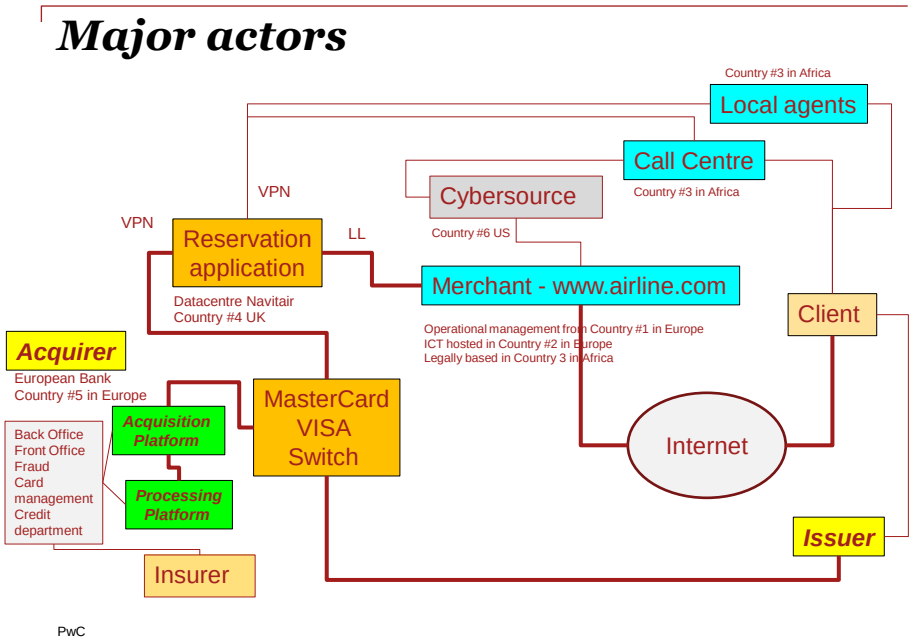

Fig. 1: Major actors involved in selling airline tickets

A client typically approaches the airline via its merchant website. Alternatively, he could contact local agents or the call centre, however the latter are not involved in the CNP fraud scenarios we discuss.

The merchant website offers a wide range of tickets and promotions, as well as opportunities for combining the plane ticket e.g. with hotel reservation or car rental, and insurance. This is a website with a content which is updated frequently, to reflect the commercial strategy of the airline.

Once a potential customer made up his mind and configured his order, the reservation application allows him to check availability and offers him the possibility to make a reservation.

Part of this reservation is requesting authorisation for credit card payment. This is requested by the reservation application to the acquirer, i.e. the merchant's bank. The acquisition platform, operated by the acquirer, will request the issuer for authorisation, i.e. whether the cardholder is valid and agrees to the transaction. Upon obtaining such authorisation, the reservation is made and the ticket will be made available to the customer.

It is important to notice that for airlines on the Africa-EU routes, it is not uncommon that the person paying for the ticket is different from the person travelling. As such, the potential control of challenging the traveller to demonstrate the credit card's presence at check-in time, is not commercially viable.

2.2 Sales process on merchant website

The airline's website is an important commercial channel. As expected, it offers a range of tickets, allowing clients the choice to book well in advance as well as « last minute ». It was based on state-of-the-art technology, but given its commercial role it did not address authenti-

cation of the customer. Such authentication is less relevant, what matters to the merchant is that the ticket is paid for, and that the traveller complies with air travel regulation. While the former is addressed through the acquiring process, the latter is addressed through the traditional channels (e.g. at the airport).

Airline Z999 was already making use of a Cybersource plug-in on its website. This plugin routes information captured during the commercial offering to a rules engine. There this information is interpreted, and used to block potentially fraudulent transactions up-front. Only those transactions that are not blocked by the rule engine make it to the actual reservation process. Rules contain elements such as black-listed IP and email addresses used by fraudsters in the past.

2.3 Reservation and payment authentication

Once the customer configured her order and made it past the anti-fraud rule engine, the airline will request authorisation from its bank to charge her credit card. The airline's bank is referred to as the acquiring bank, since it will be acquiring the transaction and later hopefully the money. The payment instruments used are governed by law, and are implemented in the schemes from e.g. VISA. The protocol that governs the communication between merchant and scheme is described in rulebooks, such as e.g. the document « Rules for VISA merchants – Cards acceptance and Chargeback management guidelines ».

In a normal case, authorisation is granted, and the transaction passes later into the subsequent states of captured and settled. However, in the case of fraud where e.g. skimmed or counterfeit cards have been used, the genuine cardholder will discover the fraudulent transaction on his statement. He will then request to reverse the transaction via his issuer, resulting in a chargeback situation that escalates to the acquirer and further on to the merchant.

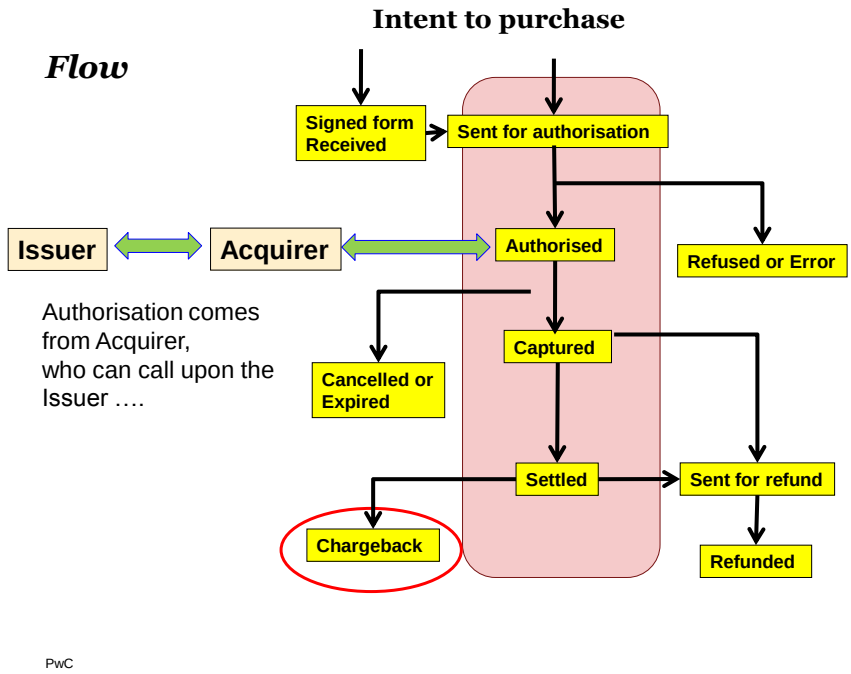

Fig. 2: Different states of a payment and their flow

To avoid such situations, at least two different payment authentication protocols have been proposed, SET (not discussed here) and 3-D Secure.

3-D Secure got his name from the fact that it structures the actors in a payment transactions in three domains. For a detailed description see [3DS]. It is also known under the brand names 'Verified By VISA', or MasterCard's 'SecureCode'. 3-D Secure's objective is payment authentication, which is the process of verifying cardholder account ownership during a purchase transaction in an online commerce environment.

The 3-D Secure model divides payment systems as follows:

- Issuer Domain—Systems and functions of the issuer and its customers (cardholders);
- Acquirer Domain—Systems and functions of the acquirer and its customers (merchants);
- Interoperability Domain—Systems, functions, and messages that allow Issuer Domain systems and Acquirer Domain systems to interoperate globally.

This can be depicted as:

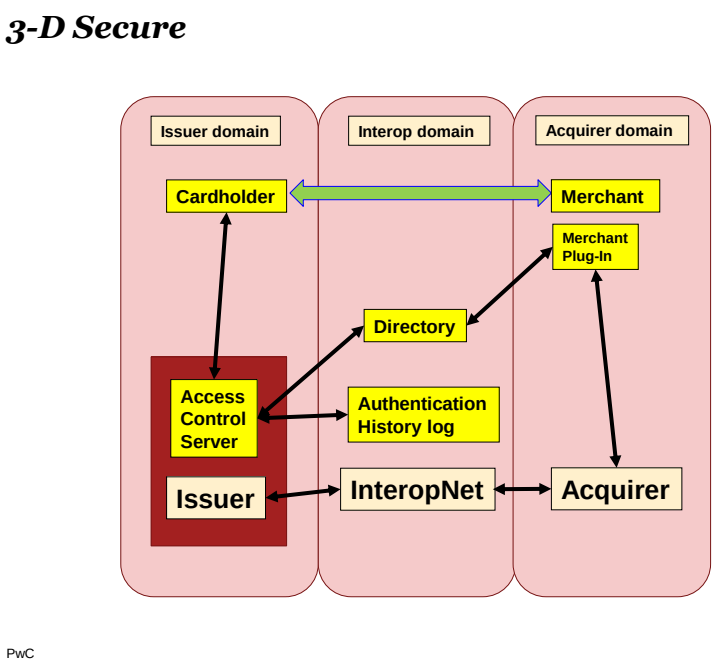

Fig. 3: 3-D Secure model – conceptual overview

For a critique of the security aspects of 3-D Secure, see for example the article by Steven Murdoch and Ross Anderson [MurAnd10].

2.4 Analysis

A merchant accepts diverse payment methods through his acquirer contract(s). The terms and conditions that the scheme imposes are reflected in the merchant/acquirer contract. Note that there is no merchant/scheme contract, everything passes through the acquirer.

3-D Secure was created as an attempt to fight a.o. CNP fraud. The idea is to shift liability towards the issuer – however implementation is complex and acceptance is slow. When an acquirer is enrolled in 3-D Secure, accepts a card, and requests authorisation of the issuer via the 3-D Secure protocol, liability shifts towards to issuer. The onus is now on the issuer to use his 3-D Secure implementation to let the card holder authenticate himself against the issuer. This should demonstrate that both card and cardholder are involved in the transaction.

However, achieving this liability shift in practise is not trivial. Scheme holders do not disclose their responsibilities and liability fully to the public or merchants. The public document *"Visa International - Operating Regulations - Volume I — General Rules - 15 November 2008"* contains the following illustrative statement in the section "About the Operating Regulations":

"In order to safeguard the security of our cardholders and merchants and the integrity of the Visa system, we have omitted certain proprietary and competitive information from this manual. As such, a reader of this manual may observe non-sequential section numbering, and information that may seem out of context or incomplete regarding the subject addressed. Visa makes no representations or warranties as to the accuracy or completeness of the text contained in this manual."

The actual responsibilities and liabilities are described in the contracts between acquirer and scheme holder, and the merchant does not necessarily have a direct link to the scheme holder. In our case there certainly was not. As such the merchant is in a weak position and may end up being liable. In the case of our client, the acquiring bank was reluctant to explain to the merchant that such liability shift was possible and preferred to claim that as per French law, an Internet sale classified as a "remote sales" and the merchant was liable in case of charge-back. The bank's representatives argued that an end-customer who disputes a payment is by default always right, and the charge back becomes a matter of discussion between merchant and customer. It is not up to the bank to get involved, it is up to the merchant to prove that the customer is wrong. Obviously, in an Internet CNP transaction such a course is unrealistic from a merchant perspective.

3 Solution

The solution consisted of a combination of legal and technical measures. First it was paramount to enforce the liability shift towards the issuer from a legal perspective. As the merchant/acquirer contract was governed by French law, and internet sales are classified as a "remote sales" ("ventes à distance") the contractual arrangements merchant/acquirer had to be amended to reflect the specific condition of credit card sales over the Internet.

Second, but in practise in parallel, the technical implementation of 3-D Secure took place. This implied that a merchant 3-D Secure plug-in was installed (referred to as the MPI – Merchant Plug-In). This MPI will route the cardholder authentication parts of the 3-D protocol to the ACS (Access Control Server) of the Issuer. This authentication can be simply password based, or alternatively it can make use of a token. Upon the protocol exchange between cardholder and issuer's Access Control Server, the issuer can conclude that has sufficient evidence

to assume the genuine cardholder is participating in the protocol. In practise, the handling of the 3-D protocol is often handled by a payment service provider (PSP).

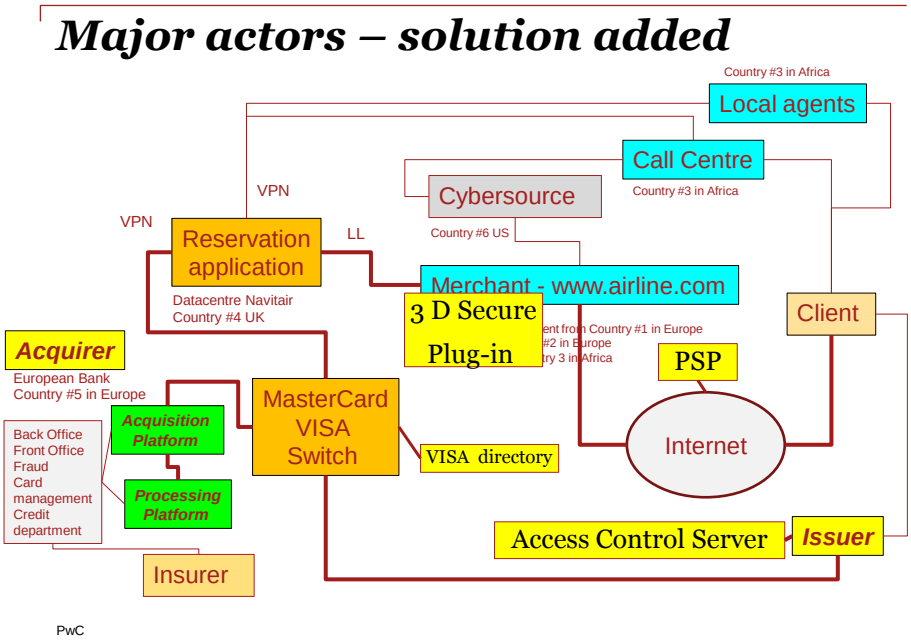

Fig. 4: Major actors involved – solution components added

4 Conclusion

Scheme holders go to great lengths to design and roll-out schemes such as 3-D Secure. While these can be critised in many ways for offering only a partial solution, it is obvious that at least they have the merit of trying to improve the situation.

Nevertheless it can be expected that a more effective and reliable solution will come from an end-to-end payment authentication created by a means under control of the cardholder.

Furthermore, it is obvious that legal alignment needs to be in place as well.

Finally it is obvious that the 3-D Secure approach did not have respect for privacy as a design criteria. This is illustrated by the fact that the transaction information gets forwarded from merchant (who does need to know the details in order to make the reservation) to acquirer (who only needs to know that the card holder is good for credit, nothing more) to the issuer (who only needs to know that his card holder wants to spent money). While cash is anonymous, when paying by credit card my bank gets all the transaction details. To make things worse, most banks outsource the handling of the 3-D protocol to a PSP, who has access to even more data because he handles transactions from multiple banks.

While Airline Z999 was happy with the results obtained, it is obvious that there remains significant room for improvement.

References

[PCIDSS] Payment Card Industry – Data Security Standard, https://www.pcisecuritystandards.org/security_standards/.

[3DS] 3-D Secure system overview, https://partnernetwork.visa.com/vpn/global/

retrieve_document.do?documentRetrievalId=119

[EMVCO] www.emvco.com

[MurAnd10] Verified by Visa and MasterCard SecureCode or, How Not to Design Authentication, Steven J. Murdoch and Ross Anderson, Financial Cryptography and Data Security, 2010, 25-28 January 2010, Tenerife.

Index

Strong authentication, card security, e-commerce, fraud, EMV.