**The “shoulder surfing case”**

**(Fraudulent withdrawals with visual capture of PIN**

**Case – May 2019)**

**KEYWORDS:**

*PSD2 — Payment services— Cash machine fraud (shoulder surfing —Gross negligence in keeping the personalized security credentials safe — Burden of proof.*

**FACTS:**

Mr B states he was the victim of pickpocketing on 17/2/2017 whilst at a train station. His stolen wallet held a debit card. He notes that he had purchased train tickets from a ticket-vending machine at the station using his bank card.

Whilst completing the transaction, he was approached by a stranger whom he believes, under the guise of providing (unsolicited) assistance, was able to capture the debit-card PIN visually as it was entered. He is emphatic that he made sure that the PIN could not be viewed as he was typing it in. Thereafter, the unknown party stayed close to Mr B whilst he was at the station waiting for his train to depart.

At 11:40 a.m. approximately, Mr B received alerts regarding transactions carried out fraudulently using his debit card, thereby alerting him to the theft.

After quickly cancelling the card, he headed to his bank and discovered that two (2) withdrawals had been made using his debit card. He vehemently denies keeping his PIN along with his card.

*He asked for the fraudulent withdrawals to be reimbursed, but the bank rejected his request.*

**LEGAL ANALYSIS:**

In that case, the client said he was a victim of shoulder surfing, a type of data theft where the attacker uses observation techniques to steal personal information or confidential information. He admitted of being approached and provided by a unsolicited assistance.

At the same time, the financial intermediary must demonstrate – according to the provisions of the law – both the authentication, the correct registration and the accounting for the payment transactions under dispute, and the absence of malfunctions in the computerized procedures; it must also prove the gross negligence of the payment card holder.

* **Legal provisions with specific reference to EU directive when applying:**

Artt. 69, par. 1, lett a) and b) and 70, par. 1, lett c), of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2); artt. 7, par 1, lett. a) and par 2, and 8 Italian Legislative decree, 15 December 2017, n. 218, implementing Directive (EU) 2015/2366 on payment services in the internal market.

**LEGAL SOLUTION:**

This case required a determination of whether the client used the requisite degree of care with respect to safeguarding his or her PIN for a debit or credit device (Art. 7, Legislative Decree no. 11/2010). The Arbitro bancario e finanziario (ABF) states that the client admission of having being victim of shoulder surfing is not sufficient, in itself, to prove the gross negligence of the cardholder: the techniques for stealing personal identification codes are increasingly sophisticated and make it possible for third parties to acquire the codes through no fault of the customer (Roma Panel, dec. 23/2015).

Plus, on our side, the client that the fraudulent use of the device was made possible by the furtive, visual retrieval of the PIN as it was entered. Proof came in the form of the actual use of the card to purchase tickets at the station.

However, the ABF also found that the card user must take special care to keep his or her PIN secret. This is the principal line of defence against unauthorized use.

(Naples Panel, dec. 6848/2015).

**SUGGESTED SOLUTION:**

Pros and cons of the client's position. The recommendation is to apply for a hearing before the Arbiter, emphasizing the care taken by the cardholder as they entered their PIN. Seek out any available evidence (e.g. surveillance video footage).