**“Mrs Y case”**

**(Sim Swap Scam – May 2020)**

**KEYWORDS:**

*PSD2 — Payment services — Sim swap scam — Strong customer authentication — Burden of proof — Identity thief — On-line banking account fraud — Independence of the elements* *of strong customer authentication.*

**FACTS:**

Mrs Y states that on 25/07/2019, around 5 p.m., she realised that her mobile phone had become inactive; the morning after (26/07/2019), as the problem persisted, she attempted to contact her mobile provider's customer-service line. She was told that the Sim card had been de-activated at her request. The customer, with no knowledge of that request, asked that her Sim be reactivated, which it was, a short time later. Following the Sim being reactivated, the bank-account holder received two text messages from the bank, dated 25/07/2019. In the first, received at 5:31 p.m., the Bank provided a notice of the mobile-token service being activated; with the second, which was time-stamped 7:30 p.m., the bank sent an alert, requesting the customer contact the bank if the service in question had not been requested by the customer. The customer, who had never requested such service be activated, contacted her bank using the toll-free number, and reviewed the transaction list on her bank account. She saw an unauthorised withdrawal in the amount of Euro 4,992.00, dated 25/7/2019, made at an ATM without using a bank card. The account holder said she had never disclosed or shared her online-banking credentials, and that she had only ever accessed online banking using the website or the intermediary's official app. The customer also noted that she found a telephone number (other than the one registered on the portal) to which the codes had been sent by the bank intermediary.

*The customer therefore believes herself to be the victim of a “Sim swap scam”. In response to her request to be indemnified of the amounts fraudulently withdrawn, the customer received an offer of a 50% reimbursement from the Bank. The customer then contacted our legal clinic.*

**LEGAL ANALYSIS:**

The customer claims she was victim of a Sim swap fraud, a scam which does not require possession of a debit card: a person's online banking credentials (customer number and secret PIN) are used instead, followed by a dynamic “one time password” (OTP), which is valid for a one-time transaction.

In that case, the bank appeared to be compliant to the PSD2 regarding the double factor authentication for the withdraw; a compliance issue with the PSD2 Directive was anyway at stake: the problem was whether the bank could be held responsible for having diverted the passcodes (OTP) to some other telephone number, without prior notification to the client.

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

Artt. 97 and 98 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. 4, 5, 6, 7, and 9 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (RTS); Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, EBA-Op-2019-06, 21 June 2019; Legislative decree, 15 December 2017, n. 218, implementing Directive (EU) 2015/2366 on payment services in the internal market.

**LEGAL SOLUTION:**

The new Sim card was issued by the telecommunication company, which is consequently responsible for the replacement to the alleged imposter. Although, the domestic interpretation of the PSD2 is that it provides strict liability regime for the payment services providers. Thus, the loss results from a lack of compliance with technical standards, since the customer did not receive any notification that the passcodes (OTP) were going to be diverted to some other number. Specifically, the bank didn’t ensure that the use of the elements of strong customer authentication is subject to measures which ensure that the breach of one of the elements does not compromise the reliability of the other elements. In fact, the bank failed in adopting security measures that are independent, in that the breach of one (the knowledge element: credentials) compromised the reliability of the other (the possession element: the Sim).

**SUGGESTED SOLUTION:**

The client declined any responsibility in giving out her security details and passcodes; nevertheless, no proof on this.

Suggestion to provide, if possible, some evidence before submitting a complaint to ABF.

**SPECIFIC REMARKS:**

Independence of the two element of SCA is a fundamental requirement under PSD2 (art. 2, n. 30) and RTS (art. 9).