**1. Phishing (Team 1, Tutor: Avv. Matteo Ghisalberti)**

1. **verify if the parties involved fall under the definition of “consumer” and “trader”:**
2. Art. 2, par. 1, n. 1, Dir. 2011/83: «any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession» « any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive».
3. *ratione personae*: Can a company be regarded as a consumer?'
4. consumer must be interpreted as referring solely to natural persons.
5. companies and association (even NGO) must be escluded

**CGCE, C-541/99 and C-542/99**: «It is thus clear from the wording of Article 2 of the Directive that a person other than a natural person who concludes a contract with a seller or supplier cannot be regarded as a consumer within the meaning of that provision»

**CGCE, C-256/00, §26**

1. *ratione materiae*, private purpose

CGCE, C-269/95 «it follows from the foregoing that, in order to determine whether a person has the capacity of a consumer, a concept which must be strictly construed, reference must be made to the position of the person concerned in a particular contract, having regard to the nature and aim of that contract, and not to the subjective situation of the person concerned. As the Advocate General rightly observed in point 38 of his Opinion, the self-same person may be regarded as a consumer in relation to certain transactions and as an economic operator in relation to others» §16

«Consequently, only contracts concluded for the purpose of satisfying an individu­ al's own needs in terms of private consumption come under the provisions designed to protect the consumer as the party deemed to be the weaker party eco­nomically. The specific protection sought to be afforded by those provisions is unwarranted in the case of contracts for the purpose of trade or professional activ­ ity, even if that activity is only planned for the future, since the fact that an activity is in the nature of a future activity does not divest it in any way of its trade or professional character» §17.

CGCE, C-464/01: goods mainly for business or for private purposes: in case of doubt, is a contract which may be attributed both to private and to trade or professional activity to be regarded as a consumer contract?

what criteria are to be applied in determining which of the private and the trade or professional purposes predominates?

L’attuale orientamento interpretativo ricostruisce lo scopo in senso oggettivo e restrittivo, in base ad indagini sull’oggetto e il contenuto del contratto, le circostanze di tempo e luogo in cui l’atto viene posto in essere.

Psd2 (dir. 2015/2366)

*Article 4*

**Definitions**

|  |  |
| --- | --- |
| 1. (30) | ‘strong customer authentication’ means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data; |

*Article 64*

**Consent and withdrawal of consent**

1.   Member States shall ensure that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the payment service provider, after the execution of the payment transaction.

2.   Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider. Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider.

In the absence of consent, a payment transaction shall be considered to be unauthorised.

3.   Consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability in accordance with Article 80. Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorised.

4.   The procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s).

*Article 69*

**Obligations of the payment service user in relation to payment instruments and personalised security credentials**

1.   The payment service user entitled to use a payment instrument shall:

|  |  |
| --- | --- |
| (a) | use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate; |

|  |  |
| --- | --- |
| (b) | notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument. |

2.   For the purposes of point (a) of paragraph 1, the payment service user shall, in particular, as soon as in receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.

*Article 72*

**Evidence on authentication and execution of payment transactions**

1.   Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.

If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

2.   Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 69. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.

*Article 73*

**Payment service provider’s liability for unauthorised payment transactions**

1.   Member States shall ensure that, without prejudice to Article 71, in the case of an unauthorised payment transaction, the payer’s payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer’s payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. Where applicable, the payer’s payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. This shall also ensure that the credit value date for the payer’s payment account shall be no later than the date the amount had been debited.

2.   Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund immediately, and in any event no later than by the end of the following business day the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

If the payment initiation service provider is liable for the unauthorised payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction. In accordance with Article 72(1), the burden shall be on the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

3.   Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and the payment service provider or the contract concluded between the payer and the payment initiation service provider if applicable.

*Article 74*

**Payer’s liability for unauthorised payment transactions**

1.   By way of derogation from Article 73, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.

The first subparagraph shall not apply if:

|  |  |
| --- | --- |
| (a) | the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or |

|  |  |
| --- | --- |
| (b) | the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced. |

The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply.

Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 69, Member States may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.

2.   Where the payer’s payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer’s payment service provider.

3.   The payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with point (b) of Article 69(1), except where the payer has acted fraudulently.

If the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under point (c) of Article 70(1), the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where the payer has acted fraudulently.

*Article 97*

**Authentication**

1.   Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

|  |  |
| --- | --- |
| (a) | accesses its payment account online; |

|  |  |
| --- | --- |
| (b) | initiates an electronic payment transaction; |

|  |  |
| --- | --- |
| (c) | carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. |

2.   With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

3.   With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users’ personalised security credentials.

4.   Paragraphs 2 and 3 shall also apply where payments are initiated through a payment initiation service provider. Paragraphs 1 and 3 shall also apply when the information is requested through an account information service provider.

5.   Member States shall ensure that the account servicing payment service provider allows the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with paragraphs 1 and 3 and, where the payment initiation service provider is involved, in accordance with paragraphs 1, 2 and 3.