Before The Arbiter for Financial Services

Case ASF 116/2023

RN ('Complainant')

Vs

APS Bank p.l.c.

Reg. No. C 2192

('Service Provider or 'APS')

Hearing of 21st December 2023

This is a complaint concerning fraudulent payments made on behalf of the Complainant to third parties from her account held with the Service Provider.

The Arbiter is dealing with several such complaints which, while differing on certain details, contain many things in common:

1. The payment will be for an amount generally under €5,000 so that it does not get blocked for exceeding the daily limit of payments agreed between the Bank and a retail customer.

2. The fraudster manages to penetrate the means of communication normally used between the Bank and the customer, usually by SMS or email.

3. The fraudster includes a link in his message and invites the customer to click on the link to make a 'validation' or 're-authentication' of his account.

4. Despite several warnings issued by the banks and the Regulator not to click on such links as Banks do not send links in their messages, and that the customer should communicate with the bank only through the official

App and/or Website through the credentials that the Bank gives to customers, the customer inattentively clicks on the link.

5. Thereafter, the fraudster somehow manages to penetrate the customer's account and make a transfer of money generally on a 'same day' basis that goes to the fraudster's account, usually, to a bank account in a Baltic country from where it is almost impossible to make an effective recall of funds once the customer reports to his Bank that it has been defrauded.

6. As a result, discord develops between the Bank and the customer as to who is responsible for bearing the burden of fraudulent payment. The customer claims that the Bank did not protect him when they allowed a communication channel normally used between the Bank and the customer to be penetrated by the fraudster and that the Bank should have noticed that it was a fraudulent payment because the customer generally does not have a history of such payments.

   The Bank maintains that the responsibility lies entirely with the customer because through gross negligence, he has given the fraudster access to his account's secret credentials and thus facilitated the fraud.

However, this particular case has special features which did not feature in most other cases even though in the end the Complainant was defrauded by a substantial amount of €19,150 representing two payments as follows:

1. Payment of €9,500 effected on 27 March 2023 at 07:30:48 hours to a certain Adam Burke

2. Payment of €9,650 effected on 28 March 2023 at 14:06:48 hours to a certain Lee Cornally (or comally).

In between these payments, three further fraudulent payments were made from her account as follows:

a. Payment of €4,500 on 27 March 2023 at 07:40:07 hours to a certain James Nolan

b. Payment of €50 on 27 March 2023 at 19:50:15 hours to the same James Nolan

c. Payment of €5,000 on 28 March 2023 at 10:59:21 hours to a certain Damien Brough.

These payments were however returned and re-credited to Complainant's account for reasons that will be elaborated hereunder. Payments a. and b. were re-credited on 28 March 2023, whereas payment c. was re-credited on 29 March 2023.[1]

On the Sunday 26 March 2023 at 12.42 hours, the day before the first payment complained of, Complainant received a message on the same SMS number she normally receives messages from APS stating:

> *"we are about to impose a hold on your account and remove your device, to avoid this pass security here at https://myaps-bank.com".*[2]

At the time, Complainant was on holiday in Portugal and during her holiday, she was receiving communications almost daily from APS requesting submission of personal information and documentation related to a home loan application which was being considered by APS and which also involved a change from Valletta to Swatar branch.

The Complainant admitted:

> *"I clicked on that link as instructed which took me to a website with a mirrored near-identical format to myAPS online domain, where I was prompted to input my login credentials and confirm some personal information. Following this I received no further communication whatsoever pertaining to any transactions. Given my ongoing near-daily communication with the bank at that point in time, I believed this was a routine security check relating to the loan application and aforementioned change of branch process."*[3]

The Complainant further submitted that:

> *"never at any point during this process did I give my express authorisation to transfer any funds out of my account".*[4]

[1] Page (p.) 35; 58
[2] P. 29
[3] P. 4
[4] P. 7

This is corroborated from the timeline provided by APS[5] which confirms that on 26 March 2023 at 12:59 (i.e., a few minutes after the Complainant received the fraudulent SMS message) a One Time Password (OTP) was sent for device registration.

From evidence emanating during the hearings, as well as from similar cases heard by the Arbiter against the same Service Provider, it results that the fraudster(s) with the credentials procured fraudulently (being name, mobile number, account number, ID number and USERNAME) as well as the OTP, could register a new device that gives full access to make payments to third parties from the Complainant's account without further involvement of the Complainant, i.e., without her specific authorisation to make the payments subject of this Complaint.

It resulted that it was only on 29 March 2023 (after all 5 payments were executed and 3 of them were credited back) that the Bank attempted to contact the Complainant to enquire about the suspicious activity on her account. As the efforts to make contact on 29 March 2023 were not successful, contact was effectively made on the 30 March 2023 and, from there, the Bank agreed to start off the recall process of the fraudulent payments.[6]

The recall on the two fraudulent payments covered by this Complaint proved unsuccessful, whereas the three other payments were returned either because the account number of the beneficiary proved incorrect or because the account had in the meantime been blocked by the recipient bank.

Consequently, APS's first claim that three out of five recall requests were successful was not actually borne out by facts.

The Complainant filed a Police Report on 30 March 2023 upon her return from holiday.[7]

An official complaint was filed with the Service Provider on same day.[8]

[5] P. 58
[6] P. 61 - 62
[7] P. 31 - 33
[8] P. 13 - 18

APS replied on 19 May 2023[9] (7 weeks later) stating:

> *"we want to emphasise that our investigation has revealed that the occurrence was beyond our control and that the Bank bears no fault on its part".*[10]

This notwithstanding, the Bank offered:

> *"as a sign of good faith and in showing you compassion for your hardship",*[11]

a full and final settlement of €12,639 being 66% of the loss incurred.

Refusal of such offer led to this Complaint being filed with the Office of the Arbiter for Financial Service (OAFS) on 16 August 2023.

The official reply from the Service Provider to the Complaint was brief merely stating that they were not responsible for the fraud suffered by Complainant; that they had two-factor authentication systems in place as required by regulation; that the Complainant facilitated the fraud by giving away her credentials that gave the fraudster(s) access to her account and that any offer made and not accepted was *ex-gratia* and was no longer available.[12]

Hearings

Hearings were held on 24 October 2023,[13] 21 November 2023[14] and a further session for verbal final submissions on 15 December 2023.[15]

The parties reiterated their position as follows:

COMPLAINANT	SERVICE PROVIDER
APS were already aware on 25 March 2023, a day before the infamous SMS of this Complaint, about the SMS	*On 25 March 2023 it was during out of office hours so they decided to restrict alerts to Facebook. "We did not know*

[9] P. 19 - 20
[10] P. 19
[11] P. 20
[12] P. 41 - 42
[13] P. 43 - 50
[14] P. 63 - 69
[15] P. 70 - 76

fraud scheme and only issued warnings on their website and Facebook page rather than issue direct SMS or email warning to clients reminding them not to press links on such SMS.	*how prevalent the smishing SMS was. We received two reports and we have nearly 100,000 customers. …. It would also cost thousand and thousands of Euros, so we cannot do that every single time there is one or two reports. And the bank continually reassess which measures and levels of communication are proportionate to the potential scare … We sent emails and secure messaging to all bank customers starting 15 April and again on the 21 April"*[16]
The change of branch was taking place due to Complainant's ongoing home loan application where meetings were held at Swatar branch so that is why it was transferred there. This led Complainant to be less suspicious that SMS could be fraudulent because the Bank was regularly asking for more information. She was in contact with Swatar on 25, 27, 28, 29 March via direct call and email to discuss the home loan application as well as history of transactions on her account but during these communications the illicit activity was never flagged up. [17]	"(we) have been assisting (Complainant) with a lending *application so any discussions would have centred around that. The change of branch in this incident would not have required any further information from the customer. …. The information (Complainant) gave to the hacker, her name, her password, etc. is not information which is requested in the context of a change of branch*."[18]

[16] P. 67 - 68
[17] P. 46
[18] P. 66

After the incident, the Bank changed the procedure for changing one's device involving direct contact with client before unlocking the full functionality to the new device.[19]	APS confirm this change happened after this case.[20]
After the incident the Bank changed the daily transfer limit applicable to Complainant from €25,000 to €5,000.[21]	APS confirm default limit of €25,000 at the time of the incident was subsequently changed to €5,000 but customers can change the limit if they wish to do so.[22]
APS was nonchalant when it clearly knew that its clients were suffering fraud attacks and did not do much to protect its clients. The actions taken by APS post this incident show that even APS themselves acknowledge failure of their systems at the time of the incident.[23]	The Complainant acted in a way out of character of a *bonus pater(mater)familias* when she gave away her credentials facilitating fraudster's access to her account. Any institution could have the best system, but if clients give away their credentials their systems are bound to fail.[24]

Consultation of the Malta Communications Authority

For the Arbiter to understand the technologic intricacies on how a fraudster can personify himself like the Bank to defraud clients, he invited an expert from Bank of Valletta plc and Malta Communications Authority (MCA) security expert for consultation.

[19] P.68
[20] *Ibid*.
[21] P. 69
[22] *Ibid*
[23] P.73
[24] P.76

From the minutes of the consultation meeting,[25] it emerges that this type of fraud, technically known as *Spoofing* and *Smishing* or collectively as *Social Engineering Scams,* does not allow the Bank to take any precaution (otherwise effective warnings for customers to be careful) so that the fraudster cannot use this communication channel to defraud customers.

Analysis and consideration

For the sake of transparency and consistency, to arrive at a fair decision on such complaints, the Arbiter has published a framework model on how to apportion the responsibility for fraud between the bank concerned and the defrauded customer by taking into account factors that may be particular to each case.[26]

The model also contains several recommendations for banks to further strengthen consumer protection against increasingly capable and creative fraudsters.

But the Arbiter feels the need to strongly emphasise that while it is true that banks do not have a means of prohibiting *spoofing/smishing* in the channels of communication they use with customers, they are not doing enough to sufficiently warn customers to be careful; not to click on links contained in these messages even though it appears to be coming from the bank concerned on the medium that the bank normally uses to send messages to customers.

It is not enough to make continuous announcements on their website. It is not enough to issue warnings on mass media or social media. The consumer is busy with daily problems, and it cannot be claimed that by making a notice on the website, in the traditional media or TV, or on the bank's Facebook page, the consumer is sufficiently informed. In serious cases of such fraud, it is necessary for banks to use direct communication with the customer by SMS or email. This aspect is one of the factors included in the framework model.

On the other hand, the Arbiter understands that the fact that the client errs by clicking on a link that he has been warned not to, as it could be fraudulent, this does not automatically fall into the category of gross negligence according to

[25] These minutes can be accessed in the decisions ref and ASF 036/2023; ASF 037/2023; ASF 040/2023; ASF 041/2023; ASF 085/2023 published on OAFS website.
[26] Technical Notes | OAFS (financialarbiter.org.mt)

law. The European Court of Justice (CJEU) in the case of Wind Tre and Vodafone Italia[27] makes reference that it would not be negligent in a gross grade if it happens even to an average consumer who is reasonably informed and attentive. The Arbiter sees complaints from complainants who easily fall into this category.

After all, PSD 2 makes it clear that the consumer must give his consent to the specific payment, and it is not enough that there is general consent as contained in any Terms of Business Agreement. Banks therefore need to have a sufficiently robust payment system so that payment is not processed unless it is specifically authorised by the customer. Banks cannot escape responsibility if they leave holes in their systems whereby the fraudster can, without further involvement of the customer, make a specific authorisation of the payment in favour of the fraudster. This fact is also included in the model.

The model also considers any applicable particular circumstances of the case. There may be circumstances where the fraud message looks less suspicious. Circumstances where the customer is in negotiations for a bank loan or the customer is abroad and is carrying out transactions that are not customarily carried out by them, thus, reducing the customer's suspicion that the message received may be fraudulent.

The model also considers whether the Complainant is familiar with the bank's online payment to third-party systems by having made any similar (genuine) payment in the previous 12 months. This also helps to form an opinion on whether the monitoring of payments system which the Bank is duty bound to make (as explained in the model) is effective. [28] [29]

Decision

The Arbiter shall decide as provided for in Article 19(3)(b) by reference to what he considers to be fair and reasonable in the circumstances and substantive merits of the case.

[27] Decision 13 September 2018 C-54/17
[28] (EU) 2018/389 of 27 November 2019 RTS supplement PSD2 EU 2015/2366 Articles 2(1) and 2(2)
[29] PSD 2 EU 2015/2366 Item 68(2).

When the Arbiter applies the model proposed for this particular case, it arrives at this decision:

	Percentage of claim allocated to Service Provider	Percentage of claim allocated to Complainant
Complainant who has shown gross negligence	0%	100%
Reduction because they receive fraud message on the channel normally used by the Bank	50%	(50%)
Increase because the Complainant cooperated fully in making the complained payment	0%	0%
Increase because they had received a direct warning from the Bank in the last 3 months	0%	0%
Sub-total	50%	50%
Reduction to special circumstances[30]	20%	(20%)
Reduction for absence of similar genuine monthly payments in the last 12 months[31]	20%	(20%)
FINAL TOTAL	90%	10%

[30] The Arbiter considers there were special circumstances in this case as the Complainant was in regular contact with APS related to her bank loan and this made the fraudulent SMS less suspicious. Also, she was travelling overseas and depended on her having regular access to her bank account.
[31] P. 70

Therefore, according to the framework model, the Complainant should bear 10% of the loss and the other 90% will be borne by the Service Provider. However, the Arbiter feels that in this case, there are sufficient grounds to go beyond the model and award full 100% refund to the Complainant, for reasons explained hereunder.

The model finds that the Complainant did not continue to cooperate with the fraudster to the point of specifically authorising the fraud payments. The APS system of immediately activating a new device has enabled the fraudster to authorise the payment without further input from Complainant. It is indicative that the Bank changed the system after the event, possibly because of this and similar complaints, and included a further layer of direct identification of the customer before fully enabling the new device.

The model partially excuses the Complainant as she had not received a direct warning from APS about these fraudulent schemes in the months before this case. It is quite inexplicable why the Service Provider waited 3 weeks before issuing such direct alerts to its client via SMS and email when it would have been prudent to assume that there was more fraud in the works than the two cases reported to them by the 25 March 2023. The argument that these would be disproportionate and would cost thousands of Euros is almost offensive.

Furthermore, the Arbiter has to remark that the payments monitoring systems of the Service Provider proved somewhat deficient in this event especially in allowing the 5th payment for €9,650 to go through on the 28 March 2023[32] after the 2nd payment effected the previous day for €4,500 had already been returned (incorrect account number).[33]

Furthermore, allowing a flat, across-the-board €25,000 transaction limit even applicable to retail clients was at best disingenuous of the Service Provider and has clearly facilitated the size of this loss compared to other cases related to banks that adopt more prudent transaction limits.

[32] P. 35
[33] P. 62

Thus, in terms of Article 26(3)(c)(iv) of Cap. 555 of the Laws of Malta, the Arbiter is ordering APS Bank p.l.c. to pay the Complainant the sum of nineteen thousand, one hundred and fifty Euros (€19,150).

Payment must be made within five working days of the date of the decision. Otherwise, legal interest starts to run from the expiry of the five days to the date of effective payment.

Expenses[34] of this case are to be borne by the Service Provider.

Alfred Mifsud
Arbiter for Financial Services

[34] Arbiter expects that for an ADR mechanism, expenses should be lower than those applicable for a civil/commercial court.

ANNEX

A model for allocation of responsibility between Payment Service Provider (PSP) and Payment Services User (PSU) in case of payments fraud scams

Some key terms

PSP — Payment Services Provider. This can be a bank or any other financial institutions that offers payment services to customers. This document applies to all those service providers that are licensed by the MFSA, the financial regulator in Malta.

PSU — Payment Services User. This refers to any customer that receives payment services from a PSP.

PSD2 — DIRECTIVE (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.[1] This Directive is commonly referred to as PSD2 for it follows another directive also issued by the EU on the same subject.

[1] https://eur-lex.europa.eu/legal-content/EN-MT/TXT/?from=EN&uri=CELEX%3A32015L2366

Introduction

PSD2 is meant to safeguard the PSU from having responsibility for payments which are not properly authorised.

PSD2 was transposed into the Laws of Malta and adopted by the Payments Regulator, the Central Bank of Malta, by means of Directive No. 1 – THE PROVISION AND USE OF PAYMENTS SERVICES ref CBM 01/2018 which states that "***This Directive is modelled on the requisites of the Directive (EU) 2015/2366***".[2]

Preamble 72 of the PSD2 is of particular relevance to the study of allocating responsibility for fraud scam payments which are unauthorised between the PSP and the PSU. This preamble states:

> ***"In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases."***

This preamble establishes important principles in considering the said allocation of responsibility:

1. For the PSU to be responsible (s)he should not only be ordinarily negligent; PSU has to be gross negligent.
2. The onus of proof of gross negligence by the PSU falls on the PSP.
3. Any different provision (e.g., that makes PSU responsible for unauthorised payments in the absence of gross negligence) in the terms of business between the parties, shall be null and void.

[2] Directive-1.pdf (centralbankmalta.org)

In terms of preamble 71 of the said PSD2, the PSU shall be responsible for payment of any unauthorised payment transaction only up to a limit of €50, unless the PSU has acted fraudulently or with gross negligence.

Gross negligence is not specifically defined in PSD2, and each case would have its own merits to determine whether the PSU has contributed to the loss through gross negligence. Most complaints filed with the Arbiter related to fraud payment scams are between PSPs that attribute gross negligence to PSUs, and PSUs denying such gross negligence.

The preamble in PSD2 gives only one example of gross negligence (where the device and the authenticating codes are kept together and negligently made available to fraudsters), but fraud has become much more sophisticated than was the case when PSD2 was promulgated. Determining the presence or absence of gross negligence has become much more challenging as the circumstances of each scam tend to follow the same pattern but differ in important peculiarities.

The Arbiter strongly maintains that the choice between ordinary negligence and gross negligence is not binary. It is not the case that ordinary negligence means no responsibility whatsoever for the PSU whereas gross negligence means 100% responsibility. Between ordinary negligence and gross negligence there exists a spread of different shades of grey where it would be necessary to allocate responsibility between the PSU and PSP depending on the particular circumstances of each case. The Arbiter would suggest, in fact, that cases of zero responsibility or full responsibility to either party should be the exception rather than the rule. Preamble 73 of the PSD2 gives a strong nod to the concept of allocation of responsibility between the parties depending on whether the PSU is a consumer or a non-consumer (i.e., a business client). Such concept of allocation of responsibility should apply also in other aspects of the particular transaction.

It is important that PSPs understand that there is a difference between authentication and authorisation of payments. The general approach taken by PSPs is that once a payment is authenticated, then it is automatically authorised through the gross negligence of the PSU. This is not the case, and one needs to keep separate the concepts of authentication and authorisation.

The first general consent when signing up for a new service is not enough to authorise a payment transaction. The consent of the PSU is required every time a payment transaction is executed. Thus, it is clear that the PSU must express consent not only to the master contract agreed with the PSP but also at every single payment given to the PSP. Many PSPs outline in the terms and conditions of their framework contract that consent is provided when strong customer authentication (SCA) is applied.

SCA is an authentication process that validates the identity of the PSU or of the payment service. More specifically, the SCA indicates whether the use of the payment instrument is authorised. SCA is based on the use of at least two elements of the following three categories:

i. **Knowledge**, being something only the PSU knows (such as PIN or password);

ii. **Possession**, being something only the PSU possesses (such as a credit card or a registered device);

iii. **Inherence**, being something which the PSU is (such as the use of fingerprint or voice recognition).

Given the control systems operated by Banks through two-factor authentication (except for small payments below €50), it seems a given that payments can only be affected after being properly authenticated. However, the journey from authentication to authorisation in case of fraud payments, requires proof by the PSP that the PSU has been grossly negligent in making available to the fraudsters the payment access credentials given by the PSP as part of their terms of business relationship.

The Arbiter maintains there is no automaticity that once a fraud payment is authenticated then it is also authorised by the PSU. In fact, there may be evident circumstances when the degree of gross negligence by the PSU is diminished, if not totally eliminated. One has to bear in mind the provisions of preamble 71 of PSD2 which states that "***there should be no liability where the payer (PSU) is not in a position to become aware of the loss, theft or misappropriation of the payment instrument***".

Fraudsters are indeed getting more sophisticated in making their devious schemes hard to distinguish from innocent reality.

This raises issues on how the Arbiter is to determine the allocation of responsibility between the PSP and the PSU. In order to avoid, or at least reduce, the perception of subjectivity and inconsistency in the awards for compensation in cases of payments fraud, the Arbiter wishes to publish a model explaining the criteria, and their respective weightings, used in determining the allocation of responsibility between the PSP and the PSU.

For this purpose, the Arbiter will be adopting the following model for allocation of responsibility between the PSP and the PSU in case of fraud payments scams complaints.

The Model

Allocation of responsibility criteria *(figures in brackets indicate a reduction of responsibility)*	**PSP**	**PSU**
Unquestionable gross negligence by PSU	0%	100%
Reduction of gross negligence due to fraudster making use of normal channels of communication used by the PSP giving the clear impression of being a genuine communication – *Note 1*	50%	(50%)
Addition if PSU actively participated in the fraud beyond disclosure of credentials – *Note 2*	(30%)	30%
Addition if PSP notified PSU by direct communication to beware such scams:		
Last 3 months	(20%)	20%
Last 6 months	(10%)	10%
Over 6 months	0%	0%
Reduction if special circumstances apply – *Note 3*	20%	(20%)
Reduction if PSU made no similar genuine payments last 12 months or payment amount is untypical of PSU account experience – *Note 4*	20%	(20%)

This model will have general application, but the Arbiter will be at liberty to depart from it in specific cases which require particular appreciation. However, the Arbiter will justify such departures from the model with proper explanations in his decisions, where applicable.

Notes (to the table above)

Note 1: Often scammers use tactics of smishing which enable them to illegally pose as genuine communications from the PSP using their normal channel of communications including SMS, emails and phone. Even though the PSP may have no technical control to prohibit such illegalities, the PSU cannot be totally faulted for assuming it is a genuine communication. A lot depends on the effectiveness of the general educational and warnings dissemination adopted by PSP to warn their customers to beware such schemes with clear explanation of what and what not to do in the circumstances.

Note 2: Sometimes PSU go beyond simple disclosure of their security credentials, and even actively participate by going along filling payment details which should raise their awareness to the fraudulent nature of the scheme. In such case, the PSU will carry a higher dose of gross negligence.

Note 3: Special circumstances could include cases where customer is having other dealings going on with the PSP which make the fraudulent request for re-authentication less suspicious.

Note 4: PSPs are obliged to have effective monitoring systems of payments to protect their PSUs from payments frauds. Commission Delegated regulation (EU) 2018/389 of 27 November 2017 establishes regulatory technical standards for strong customer authentication and common and secure open standards of communication supplementing Directive (EU) 2015/2366.[3]

It states in article 2(1) that:

> "***Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized and fraudulent payment transactions … those mechanisms shall be based on the analyses of payment transactions taking into account elements which are typical of the payment service in the circumstances of a normal use of the personalised security credentials.***"

Article 2(2) states that the following risk-based factors have to be included in the transaction monitoring mechanisms:

a. Lists of compromised or stolen authentication elements;
b. The amount of each payment transaction;
c. Known fraud scenarios in the provision of payment services;
d. Signs of malware infection in any sessions of the authentication procedures;
e. In case the access device or the software is provided by the payment service provider, a log of the use of the access or the software provided to the payment service user and the abnormal use of the access device or the software.

It was clarified that the obligation for monitoring payments mechanisms need not be 'real time risk monitoring' and is usually carried out 'after' the execution of the payment transaction. How much after has not been defined but, obviously, for any real value of such mechanisms the space between real time payment and effective monitoring must not be long after.

[3] https://eur-lex.europa.eu/legal-content/EN-MT/TXT/?from=EN&uri=CELEX%3A32018R0389

Further, article 68(2) of PSD2 authorises a PSP to block payments:

> "***If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay.***"

If PSU never made such online payment in the 12 months before the fraud event, or if the payment is of a value untypical of ordinary experience of the PSU, consideration is given to increasing allocation to PSP for failure to adopt effective payments monitoring mechanisms.

Practical applications of the model

PSU receives an SMS on the normal channel used by the PSP to communicate with him/her informing him/her to press a link in order to validate their account. Although the PSP regularly informs through general and social media that PSU should only communicate with bank through their APP or internet banking access and should never click on links sent via email or SMS, the PSU through negligence falls for it and presses the link which seems to give him access to the normal PSP web pages that raise no suspicion of the fraud.

The fraudsters, knowing they have the PSU on hook, convinces him/her to disclose their credentials and proceed to effect payment to their own IBAN account in, say, Lithuania, changing its terms to instant/priority payment, and putting a fake beneficiary name with a Malta address (SEPA system is guided only by IBAN number and make no dynamic linking to beneficiary name).

Moments after, the PSU receives notification from the PSP that a payment was made from his/her account which the PSU believes he/she has not authorised, and for the first time he/she realises that he/she has been scammed.

Immediate report to the PSP is too late to stop the payment which was affected immediately, and a recall request proves unsuccessful.

In such a case, in the first instance, the loss gets allocated 50:50.

If there is evidence that that the PSU actually participated in the transactions by executing instructions from the fraudsters beyond disclosure of the two-factor authentication (e.g., filling the amount and last digits of beneficiary account through information obtained from the App), then the gross negligence shifts by 30% from the PSP to the PSU to become 20:80.

This is a test which takes into account the robustness of the PSPs payment security systems. Robust systems should withstand fraudulent attempts to authorise specific payments transaction, unless the PSU negligently co-operates with the fraudster beyond disclosure of security credentials and negligently co-operates with the fraudster to authorise the specific payment. If systems are not robust enough and permit a fraudster to penetrate them and authorise even without the active participation of the PSU at the level of transaction payment authority, then the PSP has to bear responsibility.

If there is evidence that PSP had in the previous three months sent direct communication (not only communication through website of general/social media) to PSU to beware such fraud schemes, then the gross negligence shifts by a further 20% from PSP to PSU. This emphasises the importance of using direct warning channels to PSUs when the PSP gets sensitive to fraud schemes being laid out to trap PSUs. In such a case, the allocation would become 0:100.

If the direct communication would have been made more than three months before but in the last six months, then the shift will be 10% so the allocation would be 10:90. If the communication would have been older than six months, no shift will be executed, and responsibility stays 20:80 always assuming active participation in the fraud transaction through gross negligence. Failing active participation (i.e., if PSU only fails by exposing the secret credentials), then the responsibility would remain 50:50 if the direct notification is older than six months.

If the fraudulent transaction happens at a time when the PSU is having dealings or negotiation with PSP on some other service which makes the fraudulent request for authentication less suspicious, this will be considered with a shift of responsibility of 20%. It may also include circumstances where PSU is making unusual use of payments, e.g., whilst travelling, which makes the fraudulent request for re-authentication less suspicious.

A further 20% similar shift will occur if PSU has never affected similar genuine online transfers in the previous 12 months, or the payment amount is way out of line of the normal account experience of the PSU, given that bank's monitoring system should be made sensitive to such abnormal events and seek validation directly from PSU before proceeding with payment.

Practical example 1

Ms AB was hit by a scam SMS while she was travelling overseas. She panicked at the prospect of her card being blocked as it was her only means to fund expenditure during her travel and she pressed the link in the SMS. The fraudster skilfully but deceptively recovered her authenticating credentials and after some 30 minutes she received an SMS from the PSP confirming payment of €4000 to a foreign IBAN account. It was then that she realised that she had been scammed and contacted the bank to block her account and to affect a recall.

As the payment was made on a priority basis by the scammer, recall proves unsuccessful even though it was promptly executed by the PSP.

The PSP refuses to refund arguing that Ms AB was grossly negligent when she pressed the link on an SMS which the bank had regular warned against on social and general media. Ms AB had made payments online in the previous 12 months but had not actively assisted the fraudster beyond negligent disclosure of her secret credentials. She had not received any direct communication of warnings about such fraud schemes from the PSP in the previous 3 or 6 months.

What portion of the blame should be carried by Ms AB?

Portion due to pressing the SMS link	50%
Add active assistance in the fraud transaction	0%
Add on if in receipt of direct warnings in the last 3/6 months	0%
Clawback: special circumstance **	0%
Clawback: no online payments previous 12 months	0%
Total allocation of responsibility	50% with 50% for the PSP

*** This case assumes normal travel In Europe and no significant unusual use of the account while travelling before the fraud event – so no special circumstance applies.*

Practical example 2

Same as above, but Ms. AB had received direct warning 2 months before.

Portion due to pressing the SMS link	50%
Active assistance in the fraud transaction	0%

Add on re receipt of direct warnings in the last 3 months	20%
Clawback: special circumstance	0%
Clawback: online payments previous 12 months	0%
Total allocation of responsibility	70% with 30% for the PSP

Practical example 3

Same as example 1 above, but Ms AB had actively assisted in the fraud by inputting data in the payment order in addition to disclosure of her secret credentials, and had received direct warning 1 month before but never made online payment in the last 12 months.

Portion due to pressing the SMS link	50%
Add on active assistance in the fraud transaction	30%
Add on re receipt of direct warnings in the last month	20%
Clawback: special circumstance	0%
Clawback: online payments previous 12 months	(20)%
Total allocation of responsibility	80% with 20% for the PSP

The Arbiter emphasises that these are examples for illustration of how the model would work in general, but always reserving the right to depart from the model if particular circumstances of a complaint so warrant, with proper explanation for such departure from the model in the case decision.

Further recommendations for PSPs to enhance their PSU protection against fraud payments scams

The Arbiter wishes to make these recommendations which should be seriously considered by PSPs.

1. Removal or reduction of standard tariff charges for recalls in case of fraud payments especially where less than 100% gross negligence applies.

2. More effective and frequent educational campaigns warning of fraud payments scams both on general and social media, but particularly using direct channels of communication with PSUs.

3. Application of this model for effecting refunds to fraud payment cases which were not complained to the OAFS but were reported to (and refused by) PSP.

4. Fixing lower online transaction limits than the overall daily limits. The Arbiter is sensitive that it is technologically challenging for PSPs to fix daily and transaction payment limits to suit each and every customer circumstance. However, it should be quite doable for PSPs to apply lower limits for retail customers than for business customers, and for the transaction limit to be lower than the daily limit which covers more than one transaction in a single day.

5. Adopting more sensitive transaction monitoring systems sensitive to unusual transactions which ought to be confirmed directly with PSU before affecting transaction.

6. Introducing stricter verification processes for changes in contact details or registering new devices (possibly including a physical visit to a branch or phone verification). Notification of such contact changes should also be sent to old contact numbers/email addresses.

7. Limiting Apps meant to generate authentication codes to only one device.