An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2022-0030
Sector:	Banking
Product / Service:	Current Account
Conduct(s) complained of:	Maladministration
Outcome:	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

On **21 September 2018**, the Complainant visited the Provider's branch and sent **€24,000** (twenty-four thousand Euro) to a third party account, via SWIFT payment. The Complainant asserts that the Provider did not exercise due diligence, with regard to the destination of the funds, in effecting this transaction.

The Complainant's Case

The Complainant held a business account with the Provider. On **21 September 2018**, the Complainant attended at the Provider's branch to transfer a sum of money to a third party via SWIFT payment. The Complainant submits that he later realised that the third party was engaged in fraudulent activity and had deceived the Complainant into transferring the funds.

Eight months later, on **28 May 2019**, the Complainant contacted the Provider seeking to retrieve the funds from the third party's account. The Provider made attempts to have the funds retrieved, but was unsuccessful in doing so.

As set out in his complaint of **24 July 2019**, the Complainant submits that:

> *"[The Provider] owed me the duty of care and should have afforded me protection by questioning me and even warning or asking me if I had carefully reviewed and researched where the transfers were going."*

In the Provider's final response letter of **16 July 2019**, the Provider stated that there was no policy of forcing customers to provide additional information before making transactions. However, the Provider's individual branches may require more information, at their own discretion, for transfers of exceptionally large sums. The Provider stated that all SWIFT transactions are screened against an industry-wide sanction list, and it says that there was no issue raised as to this transaction.

In an email to this office of **21 July 2020**, the Complainant submitted:

> *"[The Provider] may at their own discretion for exceptionally large sums require more information*
>
> *24000k (sic) would be a very large sum – what would it take to ask a question?*
> *…*
>
> *On the day of transaction the bank clerk tried (3 times) to send money she asked me are u sure information is correct. I said yes. She stood up went to talk to superior. Came back tried again and money was sent.*
>
> *Now to this day the bank have said they have no recollection of failed attempts on the transfer. I believe the reason of failed attempts where (sic) kept quiet by the bank was due to [bank] account been flagged account.*
>
> *Even during the failed attempts [Provider] still asked no questions on transfer. Zero due diligence accord and I believe the [Provider] had a duty of care to inquire more on the day on transaction (sic)."*

In an email to this office of **9 September 2020**, the Complainant reiterated his submission that the transfer failed three times before it was executed, and in particular that *"[o]n the second time we call out the numbers together*".

In an email to this office of **19 May 2021**, the Complainant submitted:

> *"We both know that monies received or sent over 10k the bank must ask questions the bank's role under government anti money laundering laws."*

/Cont'd…

The Provider's Case

In response to certain questions received by this Office on **13 July 2020**, the Provider confirmed that on 21 September 2018 the Complainant attended at a branch to transfer €24,000 to a third party.

The Provider stated that as this was a "*new instruction*", the Complainant was required to fill out a mandate for the making of the SWIFT payment, and that certain procedures were to be followed:

> *"Below is an outline of the procedure followed by branch staff when completing a swift transaction:*
>
> - *Before a transaction can be completed, a customer must provide photographic identification and written confirmation of the swift payment request. This procedure is in place to ensure the security of the customer, their account(s) and the Bank.*
>
> *When a request is received from a customer to complete a swift payment the Bank must adhere to the following procedures;*
>
> a. ***Set up:*** *Prior to processing a payment via Swift a Swift mandate must be set up. Once this Mandate has been set up it can be paid at any time by selecting the payment and entering the appropriate amount to be sent…*
>
> b. ***Mandate Indemnity:*** *Once the Bank is in receipt of a Mandate Indemnity it is kept on file for any future transactions for the specific beneficiary.*
>
> c. *Before processing/authorising a payment via swift the Bank must complete the following checks:*
>
> - *Verify signatory requirements on the account*
> - *Verify debiting account is correct*
> - *Verify payee account details are correct*
> - *If more than one mandate is set up on the account ensure that the correct one was selected*
> - *Verify that there is sufficient available funds to process the payment*
> - *If payment is in another currency verify these details are accurate*
> - *Verify the amount of the transfer requested*
> - *Verify Identification/Call confirmation on documentation*

/Cont'd…

d. ***Swift Transfer:*** *Once the above checks have been completed the authorisation form and swift mandate is printed and given to the customer to review the details and sign when satisfied all details are correct. The staff member will then process the transaction and a confirmation receipt is provided to the customer."*

The Provider submits that additional information would be sought from a customer if the Provider could not verify the required information. However, all of the information provided by the Complainant was verified, and the transaction was executed in accordance with the above procedures.

The Provider relies on page 15, heading 12, of its Terms & Conditions booklet entitled "**Payment Instructions**", which indicates that payments must be authorised by customers by the completion of instructions to the Provider.

In response to the Complainant's submission that the Provider owed him a duty of care, the Provider states that it was not responsible for errors arising from mistaken instructions, as per heading 12 of its Terms & Conditions. It submits that the Complainant was obliged to ensure that all of the information was correct, and it says that he signed the SWIFT authorisation forms and mandate form, to confirm this.

In its response to this Office the Provider submits:

> *"The Bank at all times endeavours to support customers when carrying out their transactions. However it is not within the remit of the Bank to advise a customer on whom they intend making a payment to.*
>
> *The Bank acted on the instruction of the Complainant when completing the SWIFT Transfer and any due diligence on the intended recipient of the payment was a matter for the Complainant. The Bank would not be in a position to know whether the company/customer the Complainant was sending monies to, were legitimate or otherwise."*

The Provider notes that additional questions regarding the source of the funds were not required, because the money was being debited from the Complainant's account with the Provider. The Provider submits that it was not on notice of any irregularities with the recipient account.

/Cont'd…

In the Final Response Letter of **16 July 2019**, the Provider stated:

> *"With regard to [Provider] not conducting due diligence, as the funds are for the customer to spend as they please, staff would not necessarily force customers to provide any additional information before making any transactions. The branches may at their own discretion, for exceptionally large sums, require more information for the destination of the transfer and to confirm the figure is correct, however again this is not common practice.*
>
> *As customers regularly transfer funds for the purchase of cars, houses etc. the branch would be used to seeing large transactions being processed. All SWIFT transactions are screened against an industry wide sanction list and as no issues were raised when this transaction was screened, the payments were processed as normal."*

In response to the Complainant's submission that the transaction was attempted three times by the Provider's agent, and that this indicates that the third-party account was "*flagged*", the Provider states in a submission of **3 September 2020**:

> *"The branch set up and sent the payment on the Complainant's instruction. The reason there would be an issue in the branch would be if there was missing details or the details provided were incomplete which would have prevented the staff from setting up the mandate in order to complete the payment.*
>
> *The payment went through successfully when the Complainant was in the branch. There is no record of the payment failing three times in the branch."*

When the Complainant contacted the Provider seeking to retrieve the funds from the third-party account, the Provider wrote to the third party's bank on four occasions to seek a chargeback. The recipient bank did not however respond to any of the requests.

The Complaint for Adjudication

The complaint is that in **September 2018**, the Provider wrongfully/unreasonably failed to carry out "*due diligence*" prior to/when effecting/executing the Complainant's SWIFT payment instruction.

/Cont'd…

Decision

During the investigation of this complaint by this Office, the Provider was requested to supply its written response to the complaint and to supply all relevant documents and information. The Provider responded in writing to the complaint and supplied a number of items in evidence. The Complainant was given the opportunity to see the Provider's response and the evidence supplied by the Provider. A full exchange of documentation and evidence took place between the parties.

In arriving at my Legally Binding Decision I have carefully considered the evidence and submissions put forward by the parties to the complaint. Having reviewed and considered the submissions made by the parties to this complaint, I am satisfied that the submissions and evidence furnished did not disclose a conflict of fact such as would require the holding of an Oral Hearing to resolve any such conflict. I am also satisfied that the submissions and evidence furnished were sufficient to enable a Legally Binding Decision to be made in this complaint without the necessity for holding an Oral Hearing.

A Preliminary Decision was issued to the parties on **10 September 2021**, outlining the preliminary determination of this office in relation to the complaint. The parties were advised on that date, that certain limited submissions could then be made within a period of 15 working days, and in the absence of such submissions from either or both of the parties, within that period, a Legally Binding Decision would be issued to the parties, on the same terms as the Preliminary Decision, in order to conclude the matter. Following the consideration of additional submissions from the parties, the final determination of this office is set out below.

Evidence

I note that the Complainant's SWIFT Transfer Authorisation, which is signed by the Complainant and dated **21 September 2018,** states:

> *"Subject to the general terms and conditions of my/our account, which I/We have read and accepted please carry out the instructions at my/our cost. I/We undertake to release and indemnify you and your agents from and against the consequences of any irregularity, delay from any cause whatsoever, mistake, omission or misinterpretation, that may arise and from and against any loss whatsoever including such loss which may be incurred through your agents failing properly to identify the payee named, or retaining the funds should you or your agents deem such retention expedient pending confirmation of the identity of any person involved in the transaction or the above instructions by letter or otherwise."*

/Cont'd…

I further note that the "MANDATE FOR THE MAKING OF SWIFT PAYMENTS" which is also signed by the Complainant, states:

> *"Subject to the general terms and conditions of my/our account, which I/We have read and accepted please carry out all SWIFT payments using this instruction. Payments made will be sent in the currency detailed above. I/We undertake to release and indemnify you and your agents from and against the consequences of any irregularity, delay from any cause whatsoever, mistake, omission or misinterpretation, that may arise and from and against any loss whatsoever including such loss which may be incurred through your agents failing properly to identify the payee named, or retaining the funds should you or your agents deem such retention expedient pending confirmation of the identity of any person involved in the transaction or the above instructions by letter or otherwise."*

The Provider's Terms & Conditions booklet, dated **13 January 2018**, states at page 15:

> ***"12 PAYMENT INSTRUCTIONS***
>
> *(a) You and any PISP appointed on your behalf are responsible for the accuracy of each payment instruction received by us. We are not responsible for any delay or error which arises from incomplete, unclear, inconsistent or mistaken instructions, or instructions in a form (accepted at our discretion) other than our standard form for payment instructions, which are given to or accepted by us.*
>
> *Where we are given inconsistent instructions, for example, where the receiving bank's BIC and its name and address details do not match or where the payee's IBAN is invalid or incorrect, we shall not be liable for acting in accordance with any part of those instructions.*
>
> *…*
>
> *(b) Before a payment is made from your Account, you must comply with our applicable procedures including completing, either manually or online, the relevant payment instruction or the relevant Standing Order, Direct Debit or Future Dated Payment Instruction.*
>
> *…*
>
> *(c) Before we can make a payment you must authorise the transaction by completing our relevant instruction form or by providing us with written instructions in another form which contains all of the information we require. This instruction must be signed by you or your authorised signatory in accordance with the mandate held by us. Where you use one of the Channels to authorise a transaction, you or your authorised signatory must follow whatever instructions we may give you in order to complete the instruction.*

/Cont'd…

(d) …

(e) Once received by us for execution, payment instructions are irrevocable. However, if you wish to amend or cancel an instruction that you have given us, we will use our reasonable endeavours to make such amendment or cancellation if it is possible for us to do so…"

[my underlining added for emphasis]

Analysis

The issue raised by the Complainant, which requires determination is whether the Provider had an obligation of due diligence to him, pursuant to General Principle 2.2 of the ***Consumer Protection Code 2012*** (CPC) or otherwise, requiring it to assess the legitimacy of the recipient to the transaction instructed by the Complainant, or to actively warn him in this regard.

Provision 2.2 of the CPC 2012 prescribes in that respect that a regulated entity must ensure that in all its dealings with customers and within the context of its authorisation it "*acts with due skill, care and diligence in the best interests of its customers.*"

In considering the requirements of the Provider to act with the appropriate skill, care and diligence in the circumstances which give rise to this complaint, I have considered the ***European Union (Payment Services) Regulations 2018 (S.I. No. 6/2018)*** and, in particular, Regulations 95 and 111:

"Notification and rectification of unauthorised or incorrectly executed payment transactions

95. (1) A payment service user is entitled to rectification of an ***unauthorised or incorrectly executed*** *payment transaction from a payment service provider only where the payment service user notifies the payment service provider without undue delay on becoming aware of any such transaction giving rise to a claim, including a claim under Regulation 112, and no later than 13 months after the debit date.*

(2) The time limit for notification under paragraph (1) does not apply where the payment service provider concerned has failed to provide or make available the information on the payment transaction in accordance with Part 3.

/Cont'd…

*(3) Where a payment initiation service provider is involved in an **unauthorised or incorrectly executed** payment transaction, the payment service user concerned shall obtain rectification from the account servicing payment service provider concerned pursuant to paragraph (1), without prejudice to Regulation 97(2) and (3) and Regulation 112(1) to (8).*

…

[my emphasis]

Incorrect unique identifiers

111. (1) Where a payment order is executed in accordance with a unique identifier, the payment order shall be deemed to have been executed correctly where payment is made to the payee specified by the unique identifier.

(2) Where the unique identifier provided by a payment service user is not the unique identifier of the person to whom payment was intended to be made, the payment service provider concerned shall not be liable under Regulation 112 for non-execution or defective execution of the payment transaction concerned…"

I note that the transaction at the heart of this complaint was not unauthorised or incorrectly executed. The Provider followed procedure in establishing the identity of the Complainant and verified both the account details and payee details. The instruction provided by the Complainant was executed by the Provider without error, and no issue arises as to a mistake in the unique identifier of the recipient account. Indeed, I note that the Complainant says that he and the Provider's staff members called out the numbers together, before the monies were sent to the unique identifier in question.

It seems however, that the Complainant was a victim of authorised push payment (APP) fraud. He instructed and authorised the Provider to transfer the funds to the fraudulent third party. As a result, the 2018 Regulations quoted above, have limited relevance to the issue at hand, as he authorised the Provider to proceed with the transfer in question.

I note that this situation was recently considered in the English High Court case of *Fiona Lorraine Philipp v Barclays Bank UK Plc* [2021] EWHC 10 (Comm). Although not binding in this jurisdiction, this case is nevertheless of persuasive authority.

In determining whether the Defendant bank could be held liable for a lack of due diligence in relation to an APP fraud suffered by the Plaintiff, the Court considered two of the duties owed to the Plaintiff.

/Cont'd…

The Court took the view that the bank had a primary contractual duty to act on the customer's instructions, and a subordinate duty to refrain from acting on those instructions in certain circumstances. At [77] the Court quoted the subordinate duty as laid down in *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363:

> *"The law should not impose too burdensome an obligation on bankers, which hampers the effective transacting of banking business unnecessarily. On the other hand, the law should guard against the facilitation of fraud, and exact a reasonable standard of care in order to combat fraud and to protect bank customers and innocent third parties. To hold that a bank is only liable when it has displayed a lack of probity would be much too restrictive an approach.*
>
> *On the other hand, to impose liability whenever speculation might suggest dishonesty would impose wholly impractical standards on bankers. In my judgment the sensible compromise, which strikes a fair balance between competing considerations, is simply to say that* ***a banker must refrain from executing an order if and for so long as the banker is "put on inquiry" in the sense that he has reasonable grounds (although not necessarily proof) for believing that the order is an attempt to misappropriate funds*** *of the company (see proposition (3) in* Lipkin Gorman v Karpnale Ltd (1986) [1992] 4 All ER 331 *at 349*. [1987] 1 WLR 987 *at 1006). And the external standard of the likely perception of the ordinary prudent banker is the governing one."*
>
> [Emphasis added]

The English High Court held that the Defendant bank had not been 'put on inquiry' at the time of the transaction and, at [120], that "*a bank is not to be held liable where the doubt about the genuineness of the instruction is merely speculative*". The Court therefore rejected the Plaintiff's argument that the Quincecare duty should be extended to obligate the Defendant bank to establish anti-APP policies and procedures, in circumstances where this was not required by law or banking standards. It held at [130] that this would impose "c*ertain professional standards of detective and investigative work, including potential liaison with the police*" upon the bank. I note that this Quincecare principle has been cited in this jurisdiction with approval, in *Razaq v Allied Irish Banks Plc & Aslam* [2009] IEHC 176 at [68].

In considering whether the Provider in this matter was 'put on inquiry' in the present complaint, I have had regard to the Complainant's submissions suggesting that the failed transactions show that the recipient account was 'flagged'.

/Cont'd…

I have also noted the Provider's explanation that missing or incomplete details would have prevented the mandate from being set up, and in response to the query put by this Office, the Provider says that there are no records of failed transactions, as suggested by the Complainant. Rather, the Provider has advised that:

> "We note the Complainant refers to the action of the Bank teller when she *"got up walked over to get managers approval".*
>
> Please note that the staff member required managers' approval in order to complete the transfer on the system due to the amount of funds being transferred. Prior to receiving managers' approval, the staff member did not attempt to transfer the funds."

I note that the Financial Transactions Document supplied by the Provider supports its explanation, and it does not show evidence of failed transactions. However, even if the transaction had failed, it would not automatically follow, in my opinion, that the Provider would have been on notice that the recipient account was being used as part of an APP fraud.

The Provider submits and I accept that it screened the transaction against an industry-wide sanction list, and that no issue was raised. Consequently, I do not believe that the Provider had reasonable grounds to suspect that the transaction was an attempt to defraud the Complainant. Although the Provider allowed its branch a discretion to make inquiries as to the destination of funds for exceptionally large transfers, there was no obligation on it to do so.

I do not accept that the regulatory obligation of General Principle 2.2 CPC extends to requiring the Provider to make inquiries as to the destination of funds in a situation of an authorised transfer, when the Provider is not otherwise 'put on inquiry' of potential fraud.

I am conscious that the Complainant has more recently submitted that:

> *"Since [Provider] have not bother to contact them or shown proof that they have called [the receiving bank] raised a case or fraudulent activity or have and correspondence with [the receiving bank].*
>
> *Can I please ask that ombudsman do [Provider] job and contact [the receiving bank] and raised a case.*
>
> *This account is more then likely still active steeling money each day of others! Now [Provider] could not care less about fraud or there costumers lied and withheld information from me on this case I'm asking the ombudsman to reach out to [the receiving bank]."*

/Cont'd…

The Provider, in its response to this investigation, has referred to four separate SWIFT messages it sent to the recipient bank during May and June 2019, but none of which led to the return of funds. On 15 November 2021, the Provider supplied details of how the SWIFT system operates, as between banks, and again pointed to the contents of the messages it had sent to the receiving bank, by way of confirmation of the efforts it had gone to on behalf of the Complainant, to seek to retrieve his monies. It confirmed that the receiving bank did not respond to those messages.

This evidence and the SWIFT message reference number has enabled the Complainant to further pursue this matter directly with the receiving bank, though I note the difficulties he has mentioned in securing a response from the recipient bank which is in another juridiction.

It should be noted that it would not be appropriate for the FSPO to communicate with the recipient bank on behalf of the Complainant. As the impartial adjudicator of complaints, it would not be appropriate for this Office to seek to act on behalf of the respondent Provider, or to act on behalf of the Complainant, regarding the matter he has raised.

Insofar as this complaint is concerned, that in **September 2018**, the Provider wrongfully/unreasonably failed to carry out "*due diligence*" prior to/when effecting/executing the Complainant's SWIFT payment instruction, I take the view on the evidence available, details of which are referenced above, that the complaint cannot be upheld. I am satisfied that the Provider acted in accordance with its Terms & Conditions by carrying out the instructions given to it by the Complainant, and I am also satisfied that the Complainant was responsible for the consequences of giving those instructions to the Provider.

Accordingly, I do not accept that the Provider wrongfully or unreasonably failed in an obligation of due diligence, when executing the Complainant's authorised transaction, and for the reasons outlined above, this complaint is not upheld.

Conclusion

My Decision, pursuant to ***Section 60(1)*** of the ***Financial Services and Pensions Ombudsman Act 2017***, is that this complaint is rejected.

/Cont'd…

The above Decision is legally binding on the parties, subject only to an appeal to the High Court not later than 35 days after the date of notification of this Decision.

MARYROSE MCGOVERN
Deputy Financial Services and Pensions Ombudsman

25 January 2022

Pursuant to *Section 62* of the *Financial Services and Pensions Ombudsman Act 2017*, the Financial Services and Pensions Ombudsman will publish legally binding decisions in relation to complaints concerning financial service providers in such a manner that—

(a) ensures that—
(i) a complainant shall not be identified by name, address or otherwise,
(ii) a provider shall not be identified by name or address,
and
(b) ensures compliance with the Data Protection Regulation and the Data Protection Act 2018.