



<u>Decision Ref:</u>	2021-0113
<u>Sector:</u>	Banking
<u>Product / Service:</u>	Money Transfer (between accounts/between banks/3rd)
<u>Conduct(s) complained of:</u>	Handling of fraudulent transactions Dissatisfaction with customer service Failure to process instructions in a timely manner Failure to provide adequate security measures
<u>Outcome:</u>	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

The complaint concerns a transfer of funds from a current account.

The Complainant's Case

The Complainant says that on **2 March 2020** he visited a branch of the Provider in order to make a same day value transfer of €29,000 to a bank in the United Kingdom. He says that on **3 March 2020** he became aware that the IBAN that he had input on the same day transfer form, was fraudulent.

The Complainant states that at 17.16 on **3 March 2020** he phoned the Provider to request that the transfer be stopped or the funds frozen. The Complainant says that he spoke to the Provider's agent who advised him that the fraud department were no longer available after 5 p.m. (other than for card issues) and would contact him the following day. The Complainant states that the agent advised him to email the details to a customer service email address provided.

The Complainant says that at 22.30 on **3 March 2020** he contacted the receiving bank. He says that while the receiving bank's fraud department operates on a 24 hours basis, they advised that he would have to have the Provider's fraud department contact it directly.

The Complainant submits that earlier in the day at 18.00 on **3 March 2020** he had sought to contact the Provider's Hub Manager and left a message. The Complainant states that at 23.00 on **3 March 2020** he spoke to another Provider agent who advised that the fraud department were not available until the following day.

The Complainant states that at 08.52 on **4 March 2020** he again phoned the Hub Manager and left a message. He says that he emailed the Hub Manager and phoned twice more but received no response. The Complainant then phoned the Hub branch but the phone was not answered. The Complainant then texted the Hub Manager but received no response.

The Complainant says that shortly after 09.00 on **4 March 2020** he phoned the Provider and requested to be transferred to the fraud department but the call was not answered. The Complainant states that he then phoned the customer service department and was advised that the matter had been sent to the receiving bank. The Complainant says that the Provider rang at 09.30 to advise him of the name of the agent in the fraud department, who was looking after the issue.

The Complainant states that on a number of occasions he tried to contact the agent in the fraud department to be advised each time that he was unavailable. He says that he went to the Provider's headquarters on **4 March 2020** to request to meet with someone. The Complainant states that a member of the financial crime department met with him and advised him that the matter was being dealt with, and that the Provider had contacted the receiving bank.

The Complainant says that at 15.40 on **4 March 2020** he gave an indemnity to the Provider with regard to the transfer. He says that at 16.43 the indemnity was issued to the beneficiary Provider.

The Complainant says that on **22 April 2020**, he was advised by the Provider that the sum of **€824.55** had been lodged to his account on **20 April 2020** and that further refunds were unlikely. To his surprise he subsequently discovered that a further **€8,929** had been refunded to his account on **18 April 2020**.

The complaint is that the Provider proffered poor customer service to the Complainant after he notified it of a fraudulent transfer of funds from his account. The Complainant wants the Provider to refund the additional €19,246.45 which he did not already secure by way of refund.

The Provider's Case

The Provider, in its letter dated **25 June 2020**, states that on notification from the Complainant on 3 March 2020, it contacted the receiving bank to attempt a SWIFT recall at 17.34 that day and then via email at 17.51 and by phone at 18.00 on **3 March 2020**, to notify it of the activity. The Provider submits that it received a return email from the receiving bank on **4 March 2020** to inform it that the account had been frozen.

The Provider states that there is no agreement or legislative basis for interbank recalls for fraud, between the UK and Ireland. The Provider says that it acted in good faith on **2 March 2020**, in processing the Complainant's payment and that it had no way of identifying that the IBAN details provided by the Complainant were in any way fraudulent. It states that on receipt of the Complainant's phone call outlining the fraud, it contacted the receiving bank as soon as possible, to ask it to freeze the funds.

/Cont'd...

The Complaint for Adjudication

The complaint is that the Provider proffered poor customer service to the Complainant after he notified it of a fraudulent transfer of funds from his account.

The Complainant wants the Provider to refund €19,246.45, which he did not otherwise recover.

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 **29 March 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. In the absence of additional submissions from the parties, within the period permitted, the final determination of this office is set out below.

The Complainant in this matter was the victim of fraud whereby, unbeknownst to the Complainant, an incorrect IBAN was supplied to him by way of an email scam, known as 'redirect fraud'. This led the Complainant, at circa 11:00 am on the 2nd of March 2020, to transfer €29,000 (by way of 'same day transfer') into an account in a UK bank which was not the one into which he had intended to transfer the funds. The transfer was completed at 14:26.

The Complainant states that he apprehended this scam the following day on the 3rd of March 2020, and "*immediately*" telephoned the Provider. This phone call took place at 17:16. The Complainant ultimately recouped €9,753.55 only, leaving him at a deficit of €19,246.45. The Complainant is of the view that the manner in which the Provider dealt with the issue was substandard, and that the protocols and systems in place were deficient.

/Cont'd...

The Provider's Final Response Letter notes that, subsequent to the Complainant's phone call at 17:16 on the 3rd of March 2020, the Provider, at 17:34, attempted a recall of the transfer (communicated to the Complainant at the time, in a phone call) before contacting the bank where the recipient account was held (referred to below as 'the recipient bank') by email at 17:51 expressly requesting a "freeze on the monies".

A response was received at 17:56 suggesting a call be made to a particular phone number and the Provider duly called that number within a matter of minutes, at 18:00. A statement from the Provider's Deputy Head of its Financial Crime Unit refers to an additional phone call to a personal contact in the fraud section of the recipient bank, made between 17:34 and 17:51.

The Provider states that it "then received a return email on the 4th of March 2020 to inform us that the accounts had been frozen". This email, which responded to the Provider's email sent the previous evening at 17:51, was sent at 12:29pm on the 4th of March 2020, and advised as follows:

[redacted] has forwarded your query to me, and I can confirm that all appropriate actions have been undertaken in relation to the beneficiary account.

I have been advised that some funds may remain for recovery under indemnity – if you want to send an indemnity we will process it.

The Provider responded nine minutes later indicating that it "will of course issue an indemnity ASAP" and it requested the indemnity wording required by the recipient bank. The recipient bank provided the required wording at 15:52 and the Provider issued the formal indemnity at 16:43.

There are a number of remarks I consider it appropriate to make in relation to the foregoing. In the first place, any suggestion that the Provider failed to act promptly upon being advised by the Complainant of the fraud is simply not substantiated. The Provider issued a recall within 18 minutes of being informed of the problem and made contact with the recipient bank to notify it of the fraud and to request a "freeze" by way of email and two additional phone calls within less than 45 minutes.

In terms of communications the following day (the 4th of March 2020), the Provider promptly responded to each email from the recipient bank within nine minutes and 51 minutes respectively. I am entirely satisfied that the foregoing constituted adequate and reasonable service on the part of the Provider.

Secondly, if there was any failure to impose the freeze at an early enough time, I don't accept that responsibility for any such suggested delay can be attributed to the Provider which requested the freeze in writing, within 35 minutes of being informed of the problem. The Provider is not responsible for the actions of the recipient bank or its systems and the fact is that it could do no more than request the freeze and also promptly provide any information required by the recipient bank. I am satisfied that it did this.

/Cont'd...

Thirdly, it is not at all clear to me that any delay in imposing the freeze, resulted in the loss of funds. The freeze could not have been requested earlier in time than the point at which the fraud was reported by the Complainant, which was approximately 27 hours after the transfer had completed. The freeze was very promptly requested thereafter by the Provider. In direct response to the email requesting the freeze, the recipient bank confirmed, at 12:29pm on the 4th of March 2020, that “*all appropriate actions have been undertaken in relation to the beneficiary account*”. It was further confirmed that some funds remained for recovery.

The recipient bank’s email, quoted above, clearly implies that certain of the funds had already been dissipated by this time. Whilst the precise time when the funds were dissipated is not clear, this is not information which the Provider can supply. In addition, given the nature of the fraud perpetrated, I consider it very likely, that the funds were withdrawn very shortly after their arrival in the recipient account, and a good deal earlier than the Complainant’s phone call to the Provider, which, as already noted, was made approximately 27 hours after the transfer had completed. It seems likely that the funds which remained in the account as described in the email of at 12:29pm on the 4th of March 2020, were the funds ultimately repaid to the Complainant.

The Complainant takes specific issue with the fact that the funds were transferred to the recipient account, notwithstanding that the account name and IBAN number would not have matched. This is quite simply not a failing that can be attributed to the Provider. The Provider does not have access to the names of account holders of accounts held in other banks. The Provider simply executed the Complainant’s instructions to transfer funds to the IBAN provided by the Complainant. There was no duty or obligation on the Provider, nor could there have been, to check that the account name and IBAN matched.


In summary, whilst I have sympathy for the position of the Complainant, I do not believe that there are any grounds upon which it would be appropriate to compel the Provider to reimburse the Complainant in respect of the monies he instructed the Provider to transfer.

In light of the foregoing, and in the absence of evidence of wrongdoing by the Provider or conduct within the terms of **Section 60(2)** of the **Financial Services and Pensions Ombudsman Act 2017**. I take the view that there is no reasonable basis upon which this complaint can be upheld.

Conclusion

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

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**

22 April 2021

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.