An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2020-0326
Sector:	Banking
Product / Service:	Lodgements
Conduct(s) complained of:	Handling of fraudulent transactions
Outcome:	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

Background

The Complainant contends that the Provider acted wrongfully and unreasonably in completing a fund transfer executed by a third party to an account other than the Complainant's own, in circumstances where the name and IBAN on the transfer details did not match.

The Complainant's Case

The Complainant is a private limited company and the holder of a bank account (ending -033) with the Provider.

On **25 May 2018**, the Complainant issued an invoice to an overseas distributor, for payment of €4,380. The distributor proceeded to pay the monies, using the account details which appeared on the invoice in the understanding that these were the Complainant's account details. However, unbeknownst to it, the Complainant had been the victim of a fraud whereby its email account had been hacked and the bank details appearing on the invoice, had been amended.

When the Complainant did not receive the monies into its account, it initially queried the payment with the distributor company, which confirmed that payment had been made by it. It emailed a copy of the invoice in question to the Complainant, which upon examination by the Complainant, noticed that the IBAN details which appeared on its face were not in fact its IBAN details. Upon further investigation it was determined by the

Complainant that its emails had been hacked and fraudulent alterations had been made to the invoice in question. It subsequently complained to the Provider for its having allowed this transaction to be executed and the monies credited to the wrong account.

The Complainant company submits that, "*If the name/number combination is meaningless for a SEPA payment, the banks have a duty to inform their customers that this is so. Why do we have to fill in the "Name" box when making online transfers if it is meaningless.*"

The Complainant submits that another of its emails, which issued to a service provider in the UK, was also hacked but that a third party Bank in the UK refused to let the transfer go through, on the basis that "*the IBAN and account name do not match*".

The Complainant submits that the Provider has a responsibility to verify incoming payments with regard to the account details and the account holder's name, to prevent fraudulent activity. It submits that the Provider did not have sufficient procedures or controls in place in this regard.

The Provider's Case

The Provider has submitted that since the introduction of SEPA in 2014, all inward payments to financial institutions across Europe are IBAN driven and are not individually cross referenced against the name of the account.

The Provider notes that it did not execute the payment which is the subject matter of this dispute. Rather the payment which is the subject matter of this complaint was an inward payment to it. It confirms that it does not cross reference the name on an account for inward or outward payments but rather it validates the IBAN.

In respect of the Complainant's query as to why the name of a payee is to be included in the course of transferring monies in conjunction with an IBAN, if it has no bearing on the execution of payment, it states that the Complainant's overseas distributor completed and authorised the online transaction with their own Provider. Therefore any information requested by the distributor's own Provider when carrying out their transfer, is outside of its control.

It submits that as a Payment Service Provider, it is required by SEPA Regulation, Regulation (EU) No 260/2012, to use IBAN only as an account identifier.

It submits that the payee's name is asked for in order to facilitate further compliance with the Regulation but that notwithstanding this, the IBAN remains the account identifier for credit transfers.

The Bank confirms that its payment systems credited the funds to the IBAN provided by the Complainant's overseas distributor via their own Provider when they made this particular transfer.

/Cont'd…

The Provider notes that it was contacted by the Complainant in relation to this transaction on **01 June 2018**, and that once it became aware of this fraudulent transaction, it attempted to retrieve the funds from the third party, however, at this time there was no funds available. The Provider states that it acted in a way that meets its relevant obligations.

The Complaint for Adjudication

The complaint is that the Provider acted wrongfully and unreasonably in permitting monies to be credited to an account other than the Complainant's own in circumstances where the name and IBAN used by the payer on the funds transfer did not match.

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 **09 September 2020**, 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 Complainant, the final determination of this office is set out below.

As a Preliminary point, I would note that within the statutory framework, the ***Financial Services and Pensions Ombudsman Act 2017***, ***section 44(1)*** provides

> *Making of complaints 44.*
> *(1) Subject to section 51(2), a complainant may make a complaint to the Ombudsman in relation to the following:*

/Cont'd…

(a) the conduct of a financial service provider involving—
(i) the provision of a financial service by the financial service provider
…

The Complainant's complaint concerns an alleged breach of the Provider's duty of care, in effectively failing to provide a satisfactory financial service to it, as account holders, in not checking that the name and IBAN on a credit transfer effected by a third party matched, prior to applying it to the account which it did. No direct financial service was, however, in the circumstances, provided the Complainants.

The examination of the within complaint is conducted taking into account the foregoing considerations. I have also had detailed regard to the submissions and documentation furnished in evidence by each of the parties. I have also had regard to the relevant legislation governing the area of credit transfers.

In **May 2018**, the Complainant issued an invoice to an overseas distributor, for payment in the sum of €4,380. In making payment, the payer used the account details on the invoice which it believed had been issued to it by the Complainant. However, unbeknownst to the payer or the Complainant at the time, the Complainant had been the victim of an incidence of what is known as invoice re-direction fraud or authorized push payment fraud (APP fraud).

It seems in that regard that the invoice details of the Complainant were intercepted by the fraudster and the account details were altered, meaning that when payment was sent by the payer via its bank to the IBAN specified in the amended invoice, it went to an account other than the Complainant's.

In examining this complaint, I note that since **February 2014**, International Bank Account Numbers (IBANs) have been the sole payment account identifier for all Single Euro Payments Area (SEPA) bank accounts for national and cross-border credit transfers and direct debits in Euro, within the EU.

This is set out within Article 5 of the SEPA Regulations (Regulation (EU) No. 260/2012), as given effect to in Ireland, by S.I. No. 132/2013 - European Union (Requirements for Credit Transfers and Direct Debits in Euro) Regulations 2013, as follows:

Article 5

Requirements for credit transfer and direct debit transactions

1. *PSPs shall carry out credit transfer and direct debit transactions in accordance with the following requirements:*
(a) *they must use the payment account identifier specified in point (1)(a) of the Annex for the identification of payment accounts regardless of the location of the PSPs concerned;*

/Cont'd…

(b) they must use the message formats specified in point (1)(b) of the Annex, when transmitting payment transactions to another PSP or via a retail payment system;

(c) they must ensure that PSUs use the payment account identifier specified in point (1)(a) of the Annex for the identification of payment accounts, whether the payer's PSP and the payee's PSP or the sole PSP in the payment transaction are located in the same Member State or in different Member States…;

2. PSPs shall carry out credit transfers in accordance with the following requirements, subject to any obligation laid down in the national law implementing Directive 95/46/EC:

(a) the payer's PSP must ensure that the payer provides the data elements specified in point (2)(a) of the Annex;

(b) the payer's PSP must ensure that the payer provides the data elements specified in point 2(b) of the Annex to the payee's PSP;

…

The Annex referred to sets out the "Technical Requirements", as follows:

ANNEX
TECHNICAL REQUIREMENTS (ARTICLE 5)

(1) In addition to the essential requirements set out in Article 5, the following technical requirements shall apply to credit transfers and direct debit transactions:

(a) The payment account identifier referred to in Article 5(1)(a) and (c) must be IBAN.

..

(d) Remittance information and all other data elements provided in accordance with points (2) and (3) of this Annex must be passed in full and without alteration between PSPs in the payment chain.

(e) *Once the required data is available in electronic form payment transactions must allow for a fully automated, electronic processing in all process stages throughout the payment chain (end-to-end straight through processing), enabling the entire payment process to be conducted electronically without the need for re-keying or manual intervention. This must also apply to exceptional handling of credit transfers and direct debit transactions, whenever possible.*

…

(2) *In addition to the requirements referred to in point (1), the following requirements shall apply to credit transfer transactions:*

(a) The data elements referred to in Article 5(2)(a) are the following:
- *(i) the payer's name and/or the IBAN of the payer's payment account,*
- *(ii) the amount of the credit transfer,*
- *(iii) the IBAN of the payee's payment account,*
- *(iv) where available, the payee's name,*
- *(v) any remittance information.*

/Cont'd…

(b) The data elements referred to in Article 5(2)(b) are the following:
- *(i) the payer's name,*
- *(ii) the IBAN of the payer's payment account,*
- *(iii) the amount of the credit transfer,*
- *(iv) the IBAN of the payee's payment account,*
- *(v) any remittance information,*
- *(vi) any payee identification code,*
- *(vii) the name of any payee reference party,*
- *(viii) any purpose of the credit transfer,*
- *(ix) any category of the purpose of the credit transfer.*

The Complainant has queried why a provider requests further details from a payer, including the payee name, if it is not taken into account in the transfer. The Complainant submits that there was a duty on the Provider to cross reference the name and the IBAN prior to crediting funds to the relevant account. However, it can be seen from the above legislation that Payment Service Providers must carry out credit transfer transactions using the payment account identifier specified in point (1)(a) of the Annex, being the IBAN. It is this unique identifier which is used by Payment Service Providers for the identification of payment accounts. There is nonetheless also a requirement upon a payer's Payment Service Provider to ensure certain data, including the payee name, are obtained from the payer and furnished to the payee's Payment Service Provider under the Regulations. However this does not alter the fact that transfers are carried out using the IBAN for the identification of payment accounts and the payee Provider is not required to cross reference this information.

Incorrect unique identifiers

When an incorrect unique identifier, or IBAN, is used the relevant legislation sets out the Payment Services Provider's liability in this regard. The extent of the liability of a Payment Service Provider when an incorrect identifier has been used is set out within the Payment Services Regulations 2018 (S.*I. No. 6/2018 - European Union (Payment Services) Regulations 2018*), as follows:

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.

(3) 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—
(a) the payer's payment service provider shall make reasonable efforts to recover the funds involved in the payment transaction, and

/Cont'd…

(b) the payee's payment service provider shall cooperate in those efforts by communicating to the payer's payment service provider all relevant information for the collection of funds.

[emphasis added]

As a result, a payment order will be deemed to have been executed correctly where payment is made to the payee, as specified by the unique identifier (IBAN). In the case of incorrect payment execution, due to the use of an incorrect IBAN, the payer's Payment Service Provider must make reasonable efforts to recover the funds involved in the payment transaction and the payee's Payment Service Provider shall cooperate in those efforts, including by giving the payer's PSP all the information required to collect the funds.

Recent EU caselaw

In March 2019, the European Court of Justice (CJEU), gave judgment in the matter of *Tecnoservice Int. Srl, in liquidation v Poste Italiane SpA* (Case C-245/18), which examined the principles behind Article 74(2) of Directive 2007/64 (Payment Services Directive I) which Article related to payment orders effected by means of a bank transfer, following the input of the incorrect unique identifier by the payer.

I note that Article 74 has since been superseded by, and mirrored within, Article 88 of Directive 2015/2366 or PSD II, which in turn has been reflected in Regulation 111 of the European Union (Payment Services) Regulations 2018 [S.I. No. 6 of 2018] as set out above.

The considerations applied by the Court are therefore relevant to the current legislation. The case in question developed from a preliminary ruling request. The underlying facts are quite similar in nature to those which form the basis of the within complaint, as the case concerned a payment which had been made by a debtor of Tecnoservice, the applicant, and the transfer order executed by the payer stated the name of the account holder as well as the IBAN. However, the payer had entered the wrong IBAN into the payment order, which did not correspond to the intended payee's account, and therefore the money was received by the wrong recipient and Tecnoservice never received the monies due to it.

Tecnoservice brought an action before the Italian referring court against Poste Italiane, claiming that Poste Italiane was liable on account of its failure to check whether the IBAN indicated by the payer, corresponded to the name of the payee, and in allowing the sum in question to be transferred to the wrong recipient, despite there being sufficient information to establish that the unique identifier was incorrect.

Poste Italiane argued that it was no way liable, as it credited the account corresponding to the IBAN indicated on the order and that it was not required to carry out any additional checks whatsoever.

/Cont'd…

The referring court noted that the legislation provided that a payment order executed in accordance with a unique identifier is deemed to have been executed correctly, but it sought to ascertain from the CJEU whether the relevant provisions were applicable only to the payment service provider of the person who had ordered the payment, or whether it also applied to the payee's payment service provider.

The Court noted that from the wording of Article 74(2) did not discriminate between different types of payment service providers and that the limitation of liability provided for by that article, therefore applied to each of the providers involved in the transaction. Hence, the Court ruled that Article 74(2) must be interpreted as meaning that, when a payment order is executed in accordance with the unique identifier specified by the payment service user, which does not correspond to the payee name indicated by that user, the limitation of payment service provider liability, provided for by that article, applies to both the payer's and the payee's payment service provider.

Taking the above into account, I am satisfied that in this instance, although the unique identifier provided by the payer was not the unique identifier of the Complainant, to which payment was intended to be made, the Provider is not however liable for the execution of the payment transaction concerned.

The Complainant has pointed to the fact that the account in question, to which the monies were credited, had been "flagged" by the Provider, but that it nonetheless allowed the funds to be credited to that account. The Provider's position is that it is

> "*not in a position to comment in relation to any flags which may or may not have been applied to the recipient's account for Data Protection reasons*"

and that

> "*a payment of €4,380.00 was received by the Bank and applied to the account using the payment account identifier referred to as the International Bank account number referred to as the International Bank Account Number (IBAN). This IBAN was nominated by the payer through their own Provider."*

Ultimately, I am satisfied that it is the case that the Provider was entitled to rely on the IBAN as nominated by the payer in directing the payment to that account, bearing in mind the legislative framework which currently applies.

The Complainant, within its submissions, since the preliminary decision of this Office was issued, has queried if consideration was given to *"whether there was a duty of care for [the Provider] to inform us and all its clients that there is, in fact, no need for the name and IBAN number to match on a transaction and that extra caution is therefore required*?" I would note that on the facts before me, the payer who entered the relevant payment details and executed the payment did so via a third party provider and as a result, the Provider was not involved in this aspect of the transaction.

As it currently stands, there is no requirement upon the payer or payee bank, to cross reference the name and the IBAN. In the UK a "Confirmation of Payee" system has been

/Cont'd…

introduced, which adds an additional layer of protection before a payment is made whereby a payer will be able to verify that the account belongs to the person or business they intend to pay, before making the payment and the bank will be able to check if the name supplied matches the one holding that account. There is however, no such system currently in place in this jurisdiction.

Accordingly, whilst one must have every sympathy for the Complainant Company, given the fraud which was perpetrated, nevertheless, I do not find on the basis of the foregoing considerations, that there are any grounds upon which it would be appropriate to uphold this complaint against the Provider.

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

1 October 2020

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.