An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2021-0167
Sector:	Banking
Product / Service:	Money Transfer
Conduct(s) complained of:	Handling of fraudulent transactions Failure to provide adequate security measures Non-receipt of money
Outcome:	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

The Complainants hold a joint current account with the Provider. On **9** and **10 September 2019**, the First Complainant transferred money to a building contractor using the IBAN contained on the building contractor's invoice. It later transpired that the Complainants were the likely victims of a fraud whereby the invoice was intercepted by a third party and the IBAN details on the invoice had been changed.

The Complainants' Case

The Complainants explains that their email account was hacked by an unknown person whereby an invoice from a contractor employed to carry out works on the Complainants' home was intercepted and sent to the Complainants with alternative bank account details. The Complainants say two payments were made by Single Euro Payments Area (**SEPA**) transfer in respect of the invoice: €10,000 on **9 September 2019** and €4,050 on **10 September 2019**. In carrying out the transfer, the Complainants say they used both the name of the intended recipient and the incorrect IBAN on the SEPA request form. The Complainants say that their account, the contractor's account and the fraudulent account were all Provider accounts.

The Complainants say that there were contacted by one of the Provider's agents on **10 September 2019** asking if they had made the above payments. The Complainants say they confirmed that they made the payments *"and learnt that the monies had been defrauded."* The Complainants explain that the Provider then put a stop on their account and the following day, the Provider returned €3,890 to the Complainants' account *"which was the balance left in that account."*

The Complainants explain that they and the Provider contacted An Garda Síochána and an investigation is ongoing.

The Complainants submit that the Provider should be responsible for this type of fraud in the same way as it accepts liability for card fraud. The Complainants say the SEPA system is set up to facilitate international banking arrangements and is administrated by the Irish, and other international agencies in consort with banks, and the customer has no say in the operation. The Complainants say that for convenience and speed, banks only check the IBAN number as part of the transaction and not the name, even though they request the full details on the SEPA form.

The Complainants say this draws the consumer into a false sense of security and facilitates this type of online fraud. The Complainants explain that the UK authorities now recognise this anomaly and have changed their rules accordingly. The Complainants say that the failure on the part of the Provider to recognise the difference in the account name and the SEPA form submitted has accommodated this fraud and the Provider should therefore be liable. In addition, the Complainants say that it has been known for some time by banks that 'money mules' are being used (in particular, students with bank accounts) to perpetrate this type of fraud. The Complainants say it has been within the Provider's remit to put in place certain restrictions on accounts which do not normally carry out large transactions before they happen, but the Provider failed to do so.

Instead, the Complainants say, the Provider relies upon 'too-late monitoring', which the Complainants say does not adequately protect the consumer. The Complainants further say that they have been banking with the Provider for over 40 years and find their service and response in this instance to be far from adequate.

In a submission dated **16 August 2020**, the Complainants explained that further account details came to light during the investigation of the matter by An Garda Síochána and, arising from this, the Complainants believe that *"forensic analysis of the account and responses will show systemic failings and negligence by* [the Provider] *…"* The Complainants proceed to make the following points:

> *"a) There was a failure by the Bank to provide information to* [An Garda Síochána] *to allow them perform an early investigation. For example, why did they not contact the victims to request their permission to give their contact details to the Gardai? Without a victim, the Gardai cannot carry on an investigation. They need to advise the date of which they notified the … Gardai of the crime.*
>
> *I note that* [the Provider] *tried to contact* [a named Garda] *on 31st October last in relation to a 'court order'. This was, in fact, a standard Template Form from a Superintendent, I believe, which requested details of the fraudulent account only.*
>
> *b) Video footage was actioned by our Local Garda Station … who had received our complaint of the fraud on Sept 10th last.* [A named Garda] *requested that the Bank save the footage (normally kept for 30 days). She, in fact, had the footage collected in March 2020, and subsequently forwarded it to* [another Garda Station].

/Cont'd…

c) Account details:

[A named Garda] *has verbally told us the following:*

Within the 2-day period (9th – 10th September last) –

1) €4,000.00 was transferred from the fraudulent account to a second account (no details given.
2) Several Sterling transactions occurred via An Post.
3) Cash withdrawals via ATM / Bank counter took place.
4) The total we lost was €10,159.00.

Given published banking restrictions on personal accounts, which restrict cash withdrawals per day at €600 at ATM or €1,500 at Counter, we cannot see how the rules were followed, when over €6,000.00 cash was withdrawn over 2 days?

We believe that the Bank, rather than protect their customers, have made sure that they themselves could not suffer any losses as a result of the fraud.

We are not aware of the limitations of your investigative powers, but sincerely believe that a) Forensic evaluation of the timelines on the fraudulent account will show fault with the Bank, and b) that consultation with [a named Garda] *will show the lack of cooperation by the Bank in furthering a rapid investigation by the Gardai (which is essential in these cases).*

With regard to the SEPA payment system which had been engineered by The Banking System to cut down on the work involved for them and subsequent cost of transactions, this is predicated upon users of payment services being adequately protected against risks of fraud. Please see here under, a part of the 2015 European Directive on SEPA payments (2015/2366):

> *(7) In recent years, the security risks relating to electronic payments have increased. This is due to the growing technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and emerging types of payment services. Safe and secure payment services constitute a vital condition for a well-functioning payment services market. Users of payment services should therefore be adequately protected against such risks. Payment services are essential for the functioning of vital economic and social activities.*

We would welcome an account of the Bank's reasoning in regard to their protection measures in force at present, which apparently only recognised the fraud 'after the fact', and offers no safety net. Also, given that invoice misdirection fraud has been prevalent for years now, what measures have they taken to counter this threat to their customers? The UK Government closed the door on this type of fraud from June of 2019, so why have [the Provider] *not (even to this day)?*

/Cont'd…

Our assertion that [the Provider's] *standard SEPA request form asks for the receiving account's name as well as the IBAN number, would indicate to the user that that piece of information is used to confirm the veracity of the account. However, it is not. This is at least, misleading to the customer.*

We have suffered loss of both the €10,159.00, and €2,000 interest payable on a €10,000.00 loan @ 10% encouraged to pay the original bill. …"

The Provider's Case

The Provider says that at 10:51am on **9 September 2019**, the First Complainant made an online transfer of €10,000 which was intended for the bank account of a building and maintenance company which the Complainants had engaged to carry out certain works on their property. At 8:10am on **10 September 2019**, the Provider says the First Complainant made a further online transfer of €4,050 intended for the same contractor.

The Provider says by 10:30am on **10 September 2019**, a large portion of the recipient's account balance had been withdrawn and at 10:36am, its Fraud Prevention Unit (**FPU**) identified transactions on the recipient's account as being unusual and immediately placed a 'No Withdrawals' flag on the account. The Provider says this was to ensure that no further withdrawals by either cash or debit card were possible until the matter was investigated further. The Provider says the FPU then contacted the Incoming Payments Team by email in order to alert this team to any further possible incoming payments to the recipient's account. At 12:08pm, the Provider says the FPU emailed the Complainants' branch to inform the branch about the transactions on the Complainants' account. The FPU requested that the branch seek confirmation from the Complainants as to whether the funds had been paid to the correct (intended beneficiary) account.

The Provider says its branch telephoned the First Complainant at 13:37pm and the First Complainant confirmed that the transfers had not been intended for the account of the recipient. The Provider says that the branch emailed the FPU at 15:02pm to confirm this and that the First Complainant had reported the matter to An Garda Síochána. The Provider advises that as branch telephone calls are not recorded, it is unable to provide a recording of this call.

At 13:53pm the Provider says the recipient of the funds entered their Provider branch and approached a Teller to withdraw the remaining funds from their account. On reviewing the account transactions, the Provider says the branch staff member became suspicious and queried the source of the funds with the recipient who verbally confirmed the payments were a parental gift. The Provider says the branch staff member was not satisfied with this answer as the payment narratives on the account were to a building company, and the branch staff member also noticed the 'No Withdrawals' flag on the account. The Provider says when the staff member explained that withdrawals could not be permitted, the recipient immediately left the branch, leaving their passport behind.

/Cont'd…

The Provider says the branch staff member then placed a 'Management Hold' flag on the remainder of the funds as an additional safeguard. The Provider advises that the branch staff member telephoned the local Garda Station to explain that the recipient had left their passport at the branch when they had left the branch suddenly after being questioned about the transactions on the account. The Provider says the staff member sought guidance from the Gardaí in relation to the passport and it was explained that the branch should return the passport to the customer, should the customer request it. The Provider explains that no suspected crime was reported at this time as the branch had yet to contact the FPU for further guidance. The Provider says the Gardaí advised it would investigate the matter should it be reported by the FPU. The Provider advises that the recipient eventually collected the passport at the end of **September 2019**.

The Provider says the branch staff member telephoned the FPU to alert this department to the incident, but the time of the call cannot be confirmed, because branch calls are not recorded.

At 15:48pm, the Provider says the First Complainant emailed his branch requesting a recall of both transactions totalling €14,050 and at 16:10pm, the branch emailed the Payments Team requesting the recall. The Provider says a response was received from the Payments Team at 16:32pm outlining that as the transfers were from one Provider account to another, a recall was not dealt with by the Payments Team. The Provider says that the 'No Withdrawal' and 'Management Hold' flags which had been applied to the account had secured the balance remaining in the recipient's account at the time.

On **12 September 2019**, the Provider says the FPU emailed the recipient's branch at 11:48am to authorise the branch to debit the recipient's account balance and credit the Complainants' account with these funds. The Provider advises that it cannot provide these emails for data protection reasons and due to the criminal investigation into this matter. The Provider says the Complainants' account was credited with €3,890.39 which was the amount recouped from the recipient's account.

The Provider advises that the FPU reported this incident to An Garda Síochána under section 19 of the Criminal Justice Act, 2001 on **12 September 2019**. The Provider says the documents relating to this cannot be provided due to the criminal investigation into the matter.

The Provider says the on **12 September 2019**, the First Complainant telephoned his branch and stated that he should be compensated for the lost funds. The Provider says a complaint was logged during this call.

The Provider continues its Complaint Response by setting out the timeline of events between **18 September 2019** and **29 October 2019**.

On **18 September 2018**, the Provider says its internal records show that the Complainants' local Garda Station contacted the branch which the recipient had visited requesting that CCTV footage be preserved. The Provider says its branch staff member confirmed that a request had been sent to the Provider's Security Services Department on **11 September 2019** on the advice of the FPU.

/Cont'd…

The Provider says its branch staff member advised that the footage was available for collection on request. The Provider says the Garda asked for the telephone number for the Security Services Department and indicated that the appropriate paperwork for the CCTV request would be sent.

The Provider says that during a telephone call on **18 September 2019** with the Case Handler investigating the complaint, the First Complainant advised that he had received an email invoice from the building contractor and on noticing that the amount on the invoice was incorrect, brought this to the attention of the building contractor and another invoice with the correct amount was emailed to the First Complainant. The Provider says the First Complainant explained to the Case Handler that having checked his records, it had now been discovered that the second email he received from the building contractor had been intercepted and the IBAN details on the invoice had been amended, and the Complainants had not noticed this change before making the payments.

The Provider notes that the First Complainant telephoned its Customer Care Department twice on **24 September 2019** to speak with the Case Handler investigating his complaint but this individual was attending a meeting on each occasion. The First Complainant telephoned the Provider again on **25 September 2019** seeking an update on his complaint. The Provider says the Case Handler apologised for not being available the previous day. The Provider says it acknowledges that the Case Handler should have retuned the First Complainant's calls at the earliest opportunity on **25 September 2019** and apologises that this did not happen. During this conversation, the Provider says the Case Handler told the First Complainant that the investigation was ongoing and that due to data protection legislation, any information pertaining to the recipient or their account could not be disclosed. During a telephone call on **30 September 2019**, the Provider says this was explained again to the First Complainant who also sought an explanation as to how the Provider had permitted the recipient to open a bank account.

On **3 October 2019**, the Provider says it branch staff member who had been in contact with the Complainants' local Garda Station, emailed the Garda in question to confirm that the written request for CCTV footage had been received. However, the request was not for the branch footage of **10 September 2019** but for ATM footage of the same day. The Provider says that this would need to be requested separately.

The Provider says the Case Handler telephoned the First Complainant on **8 October 2019**, with an update on the investigation of the complaint. The Provider says the Case Handler advised that payments are IBAN driven only and are not cross referenced against account names. The Provider says it was reaffirmed by the Case Handler that no information relating to the recipient could be given to the Complainants. The Provider says the First Complainant was not satisfied with this explanation and stated that he felt the Provider could have done more by way of having adequate systems in place to cross reference IBAN numbers against account names, and on this basis the money stolen by the fraudster should be refunded by the Provider. The Provider says the First Complainant stated that the Provider's systems were set up in this matter so as to suit the Provider.

/Cont'd…

The Provider says the Case Handler apologised and empathised with the First Complainant who then requested a letter from the Case Handler outlining the Provider's provision, so that he could refer a complaint to this Office.

Also on **8 October 2019**, the Provider says its branch staff member emailed the Complainants' local Garda Station confirming the requested ATM footage had been retrieved and would be available for collection the following day. The Provider says the branch CCTV footage was collected by the Gardaí on **29 October 2019**.

The Provider says the First Complainant authorised the two payments on **9** and **10 September 2019** through its online payment option. The Provider says these payments are SEPA payments. The Provider has set out the step-by-step process for this payment method in its Complainant Response. In respect of payments 'To Another Irish Account', the Provider says the customer should select the account from which the payment is to be made and proceed to the next screen. The customer must then select the beneficiary to be paid from the list of beneficiaries already available on their account profile or enter the IBAN details of the new beneficiary. The Provider says these new details will then be saved to the customer's existing list of beneficiaries. The Provider says the customer will then input the payment amount and progress to the next screen. The Provider says a narrative can be added for the payment and the customer then confirms the payment.

The Provider says that when a customer authorises an online payment from their account to an account held by another customer with the Provider, the payment is made instantaneously. The Provider says the recipient received the two payments made by the First Complainant **on 9 September 2019** and **10 September 2019**, instantly.

The Provider says under the SEPA Scheme, all SEPA payments across Europe are IBAN driven and are not individually cross referenced against the name of the account for which a payment is intended. The Provider is required by the SEPA Regulations to use only IBAN as an account identifier. The Provider notes that in line with further requirements set out in the SEPA Regulations, it is required to obtain certain details as provided for the in Annex. As part of this, the Provider says the payee name is requested in order to facilitate compliance with the SEPA Regulations. However, the Provider explains that although it must seek the payee's name, under the SEPA Regulations, the IBAN remains the account identifier for credit transfers.

The Provider says it is aware that in the United Kingdom there is a voluntary agreement between six financial institutions to cross-reference the payee's name with the name of the beneficiary account. The Provider says this is a voluntary initiative and is not required by the SEPA Regulations. The Provider says currently, there is no regulation within this jurisdiction which directs it to apply a similar voluntary process to that which is in place in the United Kingdom. The Provider says the SEPA Regulations confirm that all payments across the 32 participating countries in Europe are IBAN driven and are not individually cross referenced against the payee named on the account. The Provider says there is no legislation or obligation in this jurisdiction for any financial service provider to introduce a system which requires IBAN and beneficiary account names be cross referenced.

/Cont'd…

The Provider says it is under no obligation to proactively contact its customers on an individual basis by email or other means to advise on the topic of fraud. However, the Provider says it continuously advertises and promotes safer ways for its customers to do banking online, with guidance and advice available on its website. The Provider also refers to section 5.5 of the Terms and Conditions for Current, Demand Deposit and Masterplan Accounts, which states:

> *'Please remember that communications made via the internet, a mobile phone or a tablet may not be secure and could be intercepted by third parties.'*

The Provider says it is ultimately the responsibility of each customer to ensure that they are providing the correct details for a transaction, as outlined in section 3.5.1, 'Payments from your Account', of the Provider's Terms and Conditions for Phone and Internet Banking. The Provider says that section 3.5.1 states as follows:

> *'You must ensure that all instructions given by you to us through [the Provider's] Phone & Internet Banking or via a third party provider are accurate and complete, and that, where appropriate, you correctly identify the Account/account (including any Unique Identifier required) to which any amount is to be credited or debited. In particular, prior to confirming any instruction to us, you must ensure that the instruction which is relayed back to you confirming the instruction that you sent through [the Provider's] Phone & Internet Banking is the instruction which you intend to give.'*

The Provider submits this illustrates that a customer must ensure that the correct Unique Identifier is given to the Provider and, in the definitions section of the Phone and Internet Banking conditions, a Unique Identifier is defined as:

> *'a combination of letters, numbers or symbols used to identify the bank account or card account of the payee when processing a payment (for example, national sort code (NSC) of the payee's bank and the payee's account number or the payee's International Bank Account Number (IBAN) and the Bank Identification Code (BIC) of the payee's bank or the payee's sixteen digit card number).'*

Referring to section 3.5.2, the Provider says once an authorised payment instruction is given by a customer, the instruction is irrevocable. The Provider says that once a payment has been authorised by a customer and executed by the Provider, there is no guarantee that the funds can be recovered, and from that point funds are recovered on a 'best efforts' basis. In addition to this, the Provider refers to section 6.25 of the Terms and Conditions for Current, Demand Deposit and Masterplan Accounts, which states:

> *'A Credit Transfer instruction cannot be cancelled or amended once we have started to process it.'*

/Cont'd…

In the Complainants' case, the Provider says it is satisfied that at 10:36am, its FPU identified the transactions on the recipient's account as being unusual and immediately placed a 'No Withdrawals' flag on the account. The Provider notes that the steps taken by the FPU were proactively taken to identify the suspicious activity on the recipient's account on **10 September 2019** in terms of the first payments to the account on **9 September 2019** and the second payment to the account on **10 September 2019**.

The Provider says that the placing of the 'No Withdrawals' and 'Management Hold' flags effectively safeguarded the remaining balance in the recipient's account, preventing further withdrawals form the account by the recipient.

The Provider says it has a number of financial crime scanning and monitoring systems which scan transactions once they have been posted to an account. These systems look at patterns, transaction types, sequences and combinations of transactions that occur on individual accounts. In addition, the Provider says it applies upfront scanning of transactions in certain instances but it cannot provide more specific details as these relate to confidential internal security policies and procedures.

The Provider advises that it reviews all of its processes and procedures on an ongoing basis and it has a number of financial crime prevention forums in place aiming to continuously improve and enhance controls. The Provider says it has not at this point in time, implemented the type of real time upfront screening that would be necessary in order to more rapidly identify this particular incident. The Provider says the solution, which is complex and challenging to design, calibrate and implement, would need to be at a low enough level to identify the two transactions in question, while at the same time ensuring that the millions of legitimate payments that are processed each day are not subject to unacceptable delays in the transfer of cleared funds to customers. The Provider says that, at an industry level, the issue is the subject of discussions with the Banking & Payment Federation Ireland which are ongoing at present, but that engagement has not reached a conclusion as of yet.

Addressing European Directive 2015/2366 on payment services, the Provider says it is satisfied that it has complied with its obligations as set out under Recital 7 in that it uses the highest levels of industry standard security, to protect customers from fraud. To ensure that customers can access their accounts over the internet with confidence, the Provider says it uses a 128-bit Secure Socket Layer encryption to protect customer information.

Additionally, the Provider says it utilises an auto time-out feature that aims to protect customers against unauthorised access. The Provider further explains that it incorporates a time and date stamp feature and each time a customer logs on to its internet banking, the application will display the details of the customer's last log-in. The Provider says it also provides customers with a Card Reader which works with a customer's debit card to provide unique security codes so that customers can make certain payments and access various online services. This provides customers with an extra security buffer from authorised or fraudulent activity.

/Cont'd…

The Provider says that customers are also required to use an 8 digit registration number and selected digits for a secure Personal Access Code in order to access its phone and internet banking system. The Provider says it utilises scanning and monitoring systems that aim to identify fraudulent transactions on accounts. These systems are designed to identify patterns, transaction types, sequences and combinations of transactions that could be fraudulent. The Provider says that these systems check and identify transactions that have been completed.

In its complaint response, the Provider has also addressed a number of the provision of the ***European Communities (Payment Services) Regulations 2018***.

The Provider says it is important to recognise that the transactions were confirmed and authorised by the First Complainant and it acted on those instructions in accordance with Regulation 88 of the Payments Services Regulations. Unfortunately, the Provider says the First Complainant provided the account details for a person the First Complainant did not intend to make the payments to. In this respect, the Provider says Regulation 111 is directly relevant and states:

> *'(1) Where a payment order is executed in accordance with the 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.'*

The Provider says that the First Complainant was fraudulently deceived into instructing the Provider to credit the bank account of the recipient. While this is an unfortunate situation and the Provider sympathises with the Complainants, the Provider says it must refer to Regulation 111(2) of the Payment Service Regulations which outlines that it will not be liable when the wrong unique identifier, the IBAN, is provided by a customer and the Provider acts in accordance with the unique identifier provided.

In terms of its dealings with An Garda Síochána, the Provider says it acted without delay and the Gardaí were contacted on **12 September 2019**, directly after the Provider had completed its preliminary investigations regarding the payments.

The Provider says it cannot supply internal records exchanged with the Gardaí. The Provider submits that it is satisfied that it co-operated fully and in line with its obligations under section 19 of the Criminal Justice Act 2011 and complied fully with the Court Orders received.

/Cont'd…

The Provider says that it empathises with the Complainants for the unfortunate position in which they find themselves. The Provider says that having conducted a full investigation, it is satisfied that it acted promptly and complied with regulation in the processing of the two payments as authorised by the Complainants. In addition, the Provider says it is satisfied that it acted promptly on **10 September 2019** in identifying the alleged fraud and raising concerns regarding the two payments which resulted in it being able to recover €3,890.39 for the Complainants. The Provider says that it encourages the Complainants to pursue the matter with An Garda Síochána and that it assures the Complainants that it will continue to fully co-operate in relation to any investigation in this regard.

The Complaint for Adjudication

The complaint is that the Provider wrongfully or unreasonably refused to reimburse the Complainants for the unrecovered balance of two transfers from the Complainants' bank account, which took place on **9** and **10 September 2019**.

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 Complainants were 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 April 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.

/Cont'd…

The SEPA Regulations

The purpose of ***European Union Regulation 260/2012*** (the **SEPA Regulations**), is to provide for cross-border, European Union wide payment services and lay down rules for credit transfers and direct debit transactions within the European Union. While the Complainants have cited Recital 7 in their submissions, I also note the following passages from Recital 8 (where PSP is an acronym for payment service provider):

> *"In the vast majority of payment transactions in the Union, it is possible to identify a unique payment account using only IBAN without additionally specifying BIC. … It seems unjustified and excessively burdensome to oblige all payers and payees throughout the Union always to provide BIC in addition to IBAN …. A much simpler approach would be for PSPs and other parties to solve and eliminate those cases where a payment account cannot be identified unambiguously by a given IBAN. Therefore the necessary technical means should be developed to enable all users to identify unambiguously a payment account by IBAN alone."*

Article 5 sets out the 'Requirements for credit transfer and direct debit transactions' and states, in relevant part, as follows (where PSU is an acronym for payment service user):

> *"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; …*
>
> *(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 …*
>
> *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 provide the data elements specified in point (2)(b) of the Annex to the payee's PSP;*
>
> *(c) the payee's PSP must provide or make available to the payee the data elements specified in point (2)(d) of the Annex."*

The Annex contained in the SEPA Regulations as referred to in Article 5 states:

> *"(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:*

/Cont'd…

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

(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.

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. …

(d) The data elements referred to in Article 5(2)(c) are the following:

(i) the payer's name,
(ii) the amount of the credit transfer,
(iii) any remittance information."

The Payment Services Regulations

In respect of the use of incorrect unique identifiers, Article 111 of the ***European Union (Payment Services) Regulations 2018***, states:

"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.

/Cont'd…

(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

(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.

(4) Where the recovery of funds in accordance with paragraph (3) is not possible, the payer's payment service provider shall provide to the payer, upon written request, all information available to the payer's payment service provider and relevant to the payer in order for the payer to issue proceedings for the recovery of the funds.

(5) Where agreed in the framework contract concerned, a payment service provider may charge the payment service user for recovery of funds.

(6) Where a payment service user provides information in addition to that specified in Regulation 69(1)(a) or Regulation 76(b)(ii), the payment service provider shall be liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user."

The Provider's Terms and Conditions

Section 5.5 of the 'Terms and Conditions for Current, Demand Deposit and Masterplan Accounts' (the **Account Terms**), states as follows:

"5.5 Please remember that communications made via the internet, a mobile phone or a tablet may not be secure and could be intercepted by third parties."

Section 6 deals with 'Making and receiving payments' and I note the following sections:

"6.23 A Credit Transfer instruction must include the information we need to identify the account you want to transfer fund to (for example, an IBAN …, a BIC …, an account number and/or sort code, or the recipient's name and address). We will tell you what details we need when you give us the instruction. …

6.25 A Credit Transfer instruction cannot be cancelled or amended once we have started to process it. …

6.52 Where we are given incomplete, unclear, inconsistent, or mistaken instruction we will not be responsible for acting in accordance with any part of those instructions or for any delay or error which arises as a result. …

/Cont'd…

6.61 …

a) you must tell us as soon as possible and without undue delay … if you believe that a payment has been made in error, was incorrectly executed, late or not properly made;

b) where we have been instructed to make a payment from your Account to an account with another financial service provider and that payment was deemed to be deficient, we will usually restore your Account as soon as possible to the state it would have been in had the payment been correctly executed. A payment is deemed to be deficient where the other financial service provider says it did not receive it, it was late or if the payment instruction is incorrectly executed by us. … We will not have any further liability to you in this respect. However, we will not do this if:

(i) we have executed the payment in accordance with the instructions provided to us or if there was a mistake in any of the details in the payment instruction provided to us; or

(ii) we can show that the payment was received by the other financial service provider;

c) where you tell us about the incorrect payment, we will make efforts to look into this and trace the payment and inform you of our findings. …"

Section 9 sets out the Provider's responsibilities to customers, as follows:

"9.1 You will have no claim against us and we will have no liability to you:

c) where your loss relates to a payment from or to your Account, or arises in connection with any payment or intended payment from or to your Account, where we could not have reasonably predicted your loss when you gave us the instruction …"

Section 3 of the applicable 'Terms and Conditions for [the Provider] Phone & Internet Banking' (the **Internet Banking Terms**), deals with 'Payments from your Account' and states, in relevant part, as follows:

*"**3.1** You authorise us to act upon any instruction to debit an Account received through* [the Provider] *Phone & Internet Banking …*

***3.5.1** You must ensure that all instructions given by you to us … are accurate and complete, and that, where appropriate, you correctly identify the Account/account (including any Unique Identifier required) to which any amount is to be credited or debited. In particular, prior to confirming any*

/Cont'd…

instruction to us, you must ensure that the instruction which is relayed back to you confirming the instruction that you sent … is the instruction which you intend to give. We are not responsible for any delay or error which arises from incomplete, unclear, inconsistent or mistaken instructions which you give us or by us accepting such instructions. Where you give us inconsistent instructions (for example, where the receiving bank's NSC or BIC and its name and address details do not match) we will not be liable for acting in accordance with any part of those instructions. We are entitled to rely on any instruction from you … and, for the avoidance of doubt, the processing by us of any such confirmed instruction shall be final and binding on you. We will not be liable for any delay or error which arises from incomplete or unclear, inconsistent and/or mistaken instructions which you give us.

3.5.2 *Once accepted by us for execution of payment instruction is 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. …"*

Formal Complaint

A formal complaint was logged during a telephone conversation with the First Complainant on **12 September 2019** which was acknowledged by the Provider by letter dated **18 September 2019**. The Provider wrote to the First Complainant on **1 October 2019** by way of update, advising him that the Provider was still investigating his complaint. The Provider issued a Final Response letter on **21 October 2019**, as follows:

"On 10 September 2019 at 10.56a.m., our Fraud Team alerted our Incoming Payments Team and our … branch to suspicious activity on the beneficiary's account. At this point, a "no withdrawals" flag was placed on the beneficiary account pending investigation. This restricted any further withdrawals from this account. Our branch staff member … contacted you to confirm these transactions, and you confirmed that the recipient was not the intended beneficiary. [The branch staff member] *confirmed this to our Fraud Team at 15.02p.m. and following further investigation it was discovered that the intended beneficiary's email had been intercepted by a third party who received the payments.*

On 15.48 p.m. you contacted [the branch staff member] *to request a recall of both of these transactions, which was done at 16.07 p.m. Our Payments Team were successful in retrieving €3,890 of the total amount transferred which was credited to your account ending 3069 on 12 September 2019.*

However, you remain dissatisfied. You want us to compensate you for the balance of €10,160. You also want clarity as to the Bank's position in relation to any possible liability and why [the branch staff member] *didn't tell you that you should initiate a recall of the money when she first initiated contact.*

/Cont'd…

I understand you want answers in relation to the beneficiary account which received the money. I want to assure you that the Bank's standard AML (Anti-Money Laundering) processes were followed in accordance with our obligations under the Criminal Justice Act, 2010 when opening this account.

Due to data protection legislation, we are unable to share any further information with you regarding the account into which the payments were made. I understand that this has caused you frustration during what can only be a difficult time. However, I assure you that once we were alerted to this matter, we acted with the utmost urgency which resulted in the retrieval of part of the money. This in itself is rare as in the majority of circumstances the money is immediately withdrawn by the fraudster as soon as it is lodged to their account.

This is a most unfortunate set of circumstances and a situation that we are seeing all too regularly. The movement of funds to third parties on the back of an email instruction with account details is fraught with danger, and all advices to the remitter are to make contact with the firm to verify and confirm the authenticity of email details. This is an essential step for the remitter to take, prior to releasing any funds to a third party following an email request.

You have been the victim of an elaborate fraud, but [the Provider] *cannot take responsibility for the release of your funds in these circumstances. We actively promote safer ways of banking on line, including the use of encrypted emails, and pointing out the necessity for a customer to be extra vigilant when they are dealing with email instructions containing account details.*

While I do not in any way want to sound dismissive, I must advise you that we cannot take this matter any further internally. Having looked into this matter, we are satisfied that when our Fraud Team became suspicious of these transactions, the Team acted swiftly in placing a "no withdrawals" flag on the beneficiary's account. Having investigated this matter thoroughly and following the correct process, we again advise that you refer the matter to the Gardaí if you haven't already done so, given fraud is a serious crime. …"

Analysis

The Complainants hired a building contractor to carry out certain works on their property. The contractor forwarded the Complainants an invoice in respect of this work at the beginning of **September 2019**, however, the incorrect amount was stated on the invoice. When sending an updated invoice, it appears that this invoice was intercepted and the contractor's IBAN was replaced with that of a third party. In paying who the First Complainant believed to be the contractor, the First Complainant transferred just over €14,000 to the third party through two credit transfers on **9** and **10 September 2019** using the third party's IBAN.

/Cont'd…

The third party account came to the attention of the Provider's Fraud Prevention Unit, FPU, on the morning of **10 September 2019** and a 'No Withdrawals' flag was placed on this account. I note that the Complainants' branch was then contacted that afternoon to request that the branch confirm the authenticity of the transfers with the Complainants.

Shortly after this, the relevant branch contacted the First Complainant where it was clarified that the third party account was not the intended beneficiary of the transfers. This information was relayed to the FPU later that afternoon.

At the same time, the third party account holder attempted to make a branch withdrawal but following certain questions from the branch staff member, did not proceed with the withdrawal. This resulted in a further flag being placed on the third party account. I note that contact was also made with An Garda Síochána and the FPU following this event.

The First Complainant emailed his branch on **10 September 2019** to request a recall of the transfers. I note that the FPU authorised the Complainants' branch to debit the third party's account balance on **12 September 2019** and to credit this amount to the Complainants' account, totalling almost €3,900.

Article 5(1) and Article 5(2) of the SEPA Regulations set out the requirements for carrying out a credit transfer. However, when processing a transfer and identifying the relevant payee, there is a distinction between the requirements of Article 5(1) and Article 5(2).

Article 5(1)(a) states, in mandatory language, that the Provider must use the IBAN when identifying the payment account. However, pursuant to Article 5(2), the Provider is required only to ensure that the Complainant provides certain data elements specified in the Annex, such as the payee's name for example. However, Article 5(2) does not state that this information is for the purpose of identifying the payee or that it must be used to identify the payee. Article 5 is clear in that the IBAN is used for the purpose of identifying the payee account and no other information is required for this purpose. It is my opinion that this is consistent with the purpose of the SEPA Regulations, and were it the intention of these Regulations to require the Provider to use payee account names or verify a payee account by reference to its name, this would have been stated in the Regulations. Further to this, Article 111(1) of the Payment Service Regulations states that when a payment order is executed in accordance with a unique identifier (such as an IBAN) the payment order is deemed to have been executed correctly where it is made to the payee specified by the unique identifier.

When it comes to transfers made on foot of an incorrect IBAN, Article 111(2) of the Payment Service Regulations provides that the Provider is not liable for the transfer when the unique identifier is provided by the Complainants. This is also reflected in section 6.52 of the Account Terms and section 3.5.1 of the Internet Banking Terms. In the circumstances of this complaint, it is my opinion that the Provider was entitled to execute the transfers by reference to the IBAN provided by the First Complainant as the unique identifier, irrespective of the other information provided by the First Complainant when authorising the transfers. Accordingly, I am not satisfied that the Provider is obliged to refund the money transferred by the First Complainant through the use of an incorrect IBAN.

/Cont'd…

The Payment Services Regulation at Article 111(3)(a) requires the Provider to make *reasonable efforts* to recover the money mistakenly transferred. Section 6.61(c) of the Account Terms states that the Provider will *"make efforts to look into this and trace the payment"*. Section 3.5.2 of the Internet Banking Terms states that

> *"if you wish to amend or cancel an instruction that you have given us,* [the Provider] *will … use our reasonable endeavours to make such amendment or cancellation if it is possible for us to do so."*

I note from the Provider's evidence that a 'No Withdrawals' flag was placed on the third party account between 10:30am and 11am on **10 September 2019** and this was followed by a 'Management Hold' flag later that afternoon. Having considered the Provider's evidence, I am satisfied these flags are likely to have prevented further withdrawal transactions from occurring on the third party account.

I also note that the initial flag was placed on the account within a very short period of the account coming to the attention of the FPU. It appears that approximately €3,900 was returned to the Complainants on **12 September 2019** following the First Complainant's recall request on the afternoon of **10 September 2019**.

It is not clear, however, whether the First Complainant was informed by the branch staff member during the telephone call at 13:37pm of the option to recall the funds and the Provider has not provided any evidence to show that any advice was given to the First Complainant regarding the possible recovery of the money.

I note that during a telephone conversation with the Case Handler on **8 October 2019**, the First Complainant raised this issue and made the point that the Provider was aware of the fraud at this point, but did not tell him to recall the funds. The First Complainant also advised the Case Hander that it was a relative who advised him to make the recall request. The Case Handler advised that she would look into this call for the First Complainant.

The Case Handler telephoned the First Complainant on **18 October 2018** having spoken to the relevant branch staff member and advised that the branch staff member could not recall whether the First Complainant was advised to recall the transfers. The Case Handler explained to the First Complainant that because the flags were already in place on the third party account, the First Complainant would not have recovered any additional funds, by recalling the funds any sooner that day.

Having considered the evidence, I am not satisfied that the First Complainant was informed of his option to recall the funds. In the circumstances, I believe it was reasonable to expect the Provider's branch staff member to have informed the First Complainant of the steps he could take to recover the money but for whatever reason, this does not appear to have occurred.

/Cont'd…

While it was explained to the First Complainant during the call on **18 October 2019** that the branch staff member did not have a recollection of advising the First Complainant about recalling the money, I note in the Final Response letter issued by the Provider, in summarising the complaint, the Provider noted that: *"You also want clarity as to … why* [the branch staff member] *didn't tell you that you should initiate a recall of the money when she first initiated contact."*

However, having considered the Final Response letter, it does not address this aspect of the complaint nor does it convey any of the information imparted to the First Complainant during the earlier telephone call. As a result, I find the Provider's Final Response letter to have been deficient given that it failed to address this aspect of the First Complainant's clear dissatisfaction with the Provider's conduct.

Notwithstanding the failure on the part of the Provider to advise the First Complainant of the option to recall the funds, I note that he emailed the Provider requesting a recall within a couple of hours of the telephone conversation with the branch staff member. In light of this and given the flag already in place on the third party account, I am not satisfied the Provider's failure in this regard is likely to have adversely impacted the amount recovered from the third party account.

Therefore, having considered the steps taken by the Provider, I believe that it made reasonable efforts to recover the Complainants' money. However, unfortunately, in this case it was not possible to recover the total amount. While this is undoubtedly disappointing for the Complainants, I do not consider that the Provider's conduct in seeking to recover the money fell below the standard which could reasonably have been expected of the Provider.

A number of telephone conversations took place between the Provider and the First Complainant between **September** and **November 2019**. I note that during these calls, the Provider's agent explained what had occurred, the type of fraud in question, that the Provider would seek to co-operate with the Complainants and the Gardaí, the steps taken by the Provider in respect of the transactions, and why it could not discuss the third party account with the First Complainant, however, certain discussions regarding the third party account did take place at a general level. I also note that the Provider has set out its interactions and involvement with An Garda Síochána. Therefore, taking the available evidence into consideration, I am satisfied that the Provider made reasonable efforts to co-operate and engage with the First Complainant and the Gardaí regarding the transfers which are the subject of this complaint.

I note that the First Complainant contacted the Provider twice on **24 September 2019** wishing to speak with the Case Handler, however she was unavailable on each occasion. The First Complainant spoke with the Case Handler the following day when she apologised for not returning the First Complainant's calls. I also note that Provider's comments that the Case Handler should have returned these calls at the earliest opportunity on **25 September 2019**.

/Cont'd…

It is clear that on **18 November 2019**, the First Complainant spoke with one of the Provider's agents regarding the progress being made in respect of the criminal investigation. The Provider's agent placed the First Complainant on hold to follow-up with the FPU. When the Provider's agent came back on the call, he advised the First Complainant that the FPU agents were unavailable at that time, but he would send an email to the relevant individuals requesting a call back to the First Complainant. However, based on the evidence presented, it is not clear if this call back was made to the First Complainant.

Since the Preliminary Decision of this Office was issued on 29 April 2021, the parties have made a number of further submissions. I have considered the Complainant's contention that

> *"There was inadequate published material directly referring to Invoice misdirection fraud (despite knowing about it for years)."*

I do not consider that this comment provides a basis for this complaint to be upheld against the provider pursuant to ***Section 60*** of the ***Financial Services and Pensions Ombudsman Act 2017,*** in the absence of evidence of wrongdoing by the Provider. Neither do I accept the relevance of arguments raised surrounding the potential to "Chargeback" a transaction undertaken, using the rules of the Visa International Scheme. I take this view because in this instance, the transactions which are the subject of the complaint, were Interpay payments in respect of which it is the SEPA rules which are instead of relevance.

Neither do I accept that the Provider can be found to be bound by the voluntary practices which have been put in place in the UK over the last number of years. In this jurisdiction the transactions at issue are governed by SEPA as detailed above, and I am satisfied that the obligations as between the parties are correctly set out within the analysis above.

Goodwill Gesture

The Provider says it recognises that the Complainants made two telephone calls to the Case Handler handling their complaint on **24 September 2019** that were not returned and it apologises for any upset or inconvenience caused. The Provider says it also wishes to apologise to the Complainants and to this Office for the delay in completing its Complaint Response. In recognition of these service failings, the Provider says it would like to offer a gesture of goodwill to the Complainants of €1,700 in full and final settlement of this complaint.

I consider this goodwill gesture to be a reasonable sum of compensation for the customer service failings on the part of the Provider. In these circumstances, on the basis that this offer remains available to the Complainants to accept, I do not propose to uphold any aspect of this complaint.

The Complainants were the unfortunate victims of a fraudulent email interception and no doubt these events have been very distressing for them. I am satisfied however that the evidence available, discloses no wrongdoing on the part of the Provider, and accordingly, the substantive complaint cannot be upheld.

/Cont'd…

Indeed, in my opinion it was the Provider's Fraud Protection Unit which quickly identified the unusual transaction pattern and was able to flag the recipient account for no withdrawals within a relatively swift period, as a result of which the Complainants succeeded in recovering some of the funds which they had inadvertently transferred to the wrong account.

In light of the compensatory offer which has been offered by the Provider and is still available to the Complainants to accept, in recognition of the Provider's poor customer service, as outlined above, neither do I consider it appropriate or reasonable to partially uphold this complaint on the basis of those more limited customer service issues. It will be a matter for the Complainants to make direct contact with the Provider, if they wish to accept that goodwill gesture, in order to conclude.

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

26 May 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.