An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2018-0079
Sector:	Banking
Product / Service:	Money Transfer (between accounts/between banks/3rd party)
Conduct(s) complained of:	Failure to advise on key product/service features
Outcome:	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

Background

The Complainant holds a student plus current account with the Provider. The Complainant asserts that the Provider is not complying with its obligations under the Single European Payments Area (SEPA) Regulation 260/2012 whereby payment service providers are obliged to offer services to all SEPA accounts on equal terms. He argues that the rules must be the same for national and cross-border transfer transactions within the European Union. The Complainant notes that the Provider requires the use of a particular form of security device to add new payees but that this requirement is waived for domestic i.e. Irish transfers under a certain threshold. He argues that this is in breach of Regulation 260/2012. The Provider denies that its policy in relation to the security device requirement or the exception for smaller domestic transfers is in breach of the Regulation and it asserts its entitlement to set security requirements as notified to and agreed by customers in its contract with them.

The Complainant's Case

In a complaint to this office, the Complainant notes that article 4(1)(a) of the SEPA Regulation 216/2014 obliges a payment service provider such as the Provider in this instance, to offer services to all SEPA accounts on equal terms so that "*the rules are the same for national and cross-border credit transfer transactions within the Union*".

He states however, that the Provider requires that a particular security device be used to add new payees, but when using the mobile app, the Provider waives this requirement for transfers less than a certain threshold but only if the destination account is an Irish account.

He states that this is a distinction that no other bank he has researched, makes. He states that the Provider rejects his contention that the Regulation obliges it any further than how it processes the transaction and maintains that it is within its prerogative to maintain different security requirements for non-Irish accounts. The Complainant does not accept that this is reasonable, proportionate, or in line with any plausible interpretation of the obligations under the Regulation in question, as well as others. He argues that it additionally hinders full competition of account Providers. He argues that the Central Bank's website uses the CPCC list of current account providers for its account switching campaign which includes a German bank in which accounts are held as German accounts. He argues that the Provider's policy effectively makes it so cumbersome to transfer even small amounts of money to such accounts as to discourage would-be switchers from using any bank not registered in Ireland. He would like this office to clarify that the Provider is obliged to provide non-discriminatory services to all SEPA accounts.

By email dated 4 April 2018, the Complainant argues that when making transfers from his account to other Eurozone accounts, he is forced to treat these as international so that there is no way to access the other Eurozone accounts without the use of the security device and other materials. He acknowledges that this has not caused him any financial loss and so he is not seeking any form of financial redress but he does not accept that the Provider's interpretation is in line with the generally accepted intention of the Regulation in question or in line with a plain reading of its text. He disagrees with the Provider's interpretation that the Regulation is restricted in scope to the charges incurred, and points to the Regulation's stated goal to create a single payment area where all payments are treated and processed on equal terms. He says that if some payments are more cumbersome than others and the sole reason is that the receiving bank is not another Irish bank, then this aim is not achieved. By email dated 24 May 2018, the Complainant declined to provide any additional evidence of support of this complaint as he stated that it was merely a point of law.

The Provider's Case

In its final response letter dated 31 August 2017, the Provider states that as a payment service provider, it is required to ensure that any scheme it uses for credit transfers complies with the Regulation and specifically with article 4(1) of Regulation 260/2012. It states that its credit transfers are governed by the SEPA Credit Transfer scheme which is a Europe wide scheme for credit transfers. It states that under the scheme rules, there is no differentiation between national payments and cross-border payments made within the EU once the payment is to an account within the SEPA zone. Consequently, it argues that the payment scheme used by the bank is in compliance with Article 4 of Regulation 260/2012. It notes that the requirement to use mobile banking or internet banking to effect a payment or the requirement to use a particular security device or not, is not governed by the SEPA scheme rules but rather are decisions that the Provider is entitled to make, having regard to its information security requirements and other regulatory obligations. It notes that the security of customer accounts is of utmost importance to it and that while it appreciates the inconvenience caused by the process, the Provider has made the decision to allow only transfers to the value of €300 to be completed on the mobile app, without the use of the security device, for security reasons.

/Cont'd…

By letter dated 3 May 2018, the Provider notes that regulation 68 of the Payment Services Regulations 2009 requires that consent to the execution of a payment is required to be provided in a manner agreed between the payer and payment service provider. The Provider argues that it considers the security requirements for execution of payments on its various digital channels on an ongoing basis having regard to all regulatory requirements and industry best practice including all European guidelines including the security of internet and mobile payments. In section 5.5.2 of the terms of conditions applicable to the Provider's current accounts (including student plus accounts), it is stated that a transaction from the account must be authorised by

> "*following whatever instructions we may give you or your authorised signatory or authorised user in relation to the operation of your Account by Cash Machine, by our internets banking service, by our telephone service and by such other Channels as we may make available from time to time*".

The Provider expresses its satisfaction that this decision does not conflict with any regulatory requirements including the provisions of Regulation 260/2012 and specifically regulation 4(1) thereof. It states that all payments are processed in accordance with the requirements of the SEPA Credit Transfer Scheme and that these rules do not speak to security requirements for executing payments. It further asserts that all scheme rules are applied equally to both domestic and cross-border payments. The Provider argues that when the Complainant opened his student plus account in September 2015, he was provided with the relevant terms and conditions which he accepted and which were emailed to him.

The Provider points to Part 4, Chapter 2 of the European Communities (Payment Services) Regulations 2009 in relation to "Single Payment Transactions" which states under provision 46 that the Chapter applies to "single payment transactions not covered by a framework contract." The Provider argues that as the Complainant's account is governed by a framework contract, and as a copy of the account terms and conditions have been provided, this chapter does not apply in the Complainant's case. The Provider points to provision 68 of the Payment Services Regulations 2009 which provides that

> "*consent to execute a payment transaction or series of payment transactions is valid only if given in the form agreed between the payer and payment service Provider concerned*" and that "*the procedure for giving consent shall be as agreed between the payer and the payment service Provider*".

The Provider concludes that it is satisfied that the complaint should not be substantiated. It states that it utilises the security device concerned to further authenticate customers facilitating the offering of greater services, including higher payment limits. It acknowledges that customers find the use of the device in question to be frustrating and indicates that it has been actively developing another security model, which would eliminate the need for the device for customers.

/Cont'd…

Decision

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

In arriving at my Legally Binding Decision I have carefully considered the evidence and submissions put forward by the parties to the complaint.

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

A Preliminary Decision was issued to the parties 9 August 2018, 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, the final determination of this office is set out below.

It should be noted from the outset that the jurisdiction of this office to consider complaints is governed by the provisions of the ***Financial Services and Pensions Ombudsman Act 2017***. Under section 44 of the 2017 Act, a Complainant can make a complaint to this office in relation to the conduct of a financial service provider involving the provision or offer of a financial service by the Provider, or the failure of a Provider to provide a particular service requested. As with other adjudicative bodies, it is not appropriate (or in my view, permissible) for this office to consider hypothetical arguments in relation to potential ramifications of a particular policy as applied by a regulated financial service provider. The jurisdiction of this office is limited to the investigation of complaints as set out in section 44. In the context of the present complaint, this means that this investigation can only consider whether the actions of the Provider in the present case (in requiring the use of the security device in question to add payees for domestic credit transfers of amounts above the relevant threshold or to add payees for all transfers elsewhere in the Eurozone) can be upheld for any of the reasons listed in section 60(2) of the 2017 Act, such as whether the relevant conduct is contrary to law. This decision does not offer any view as to whether the policy of the Provider is or could be contrary to law or anti-competitive as applied to other, unidentified individuals or financial institutions.

/Cont'd…

The Single Euro Payments Area (SEPA) initiative creates an integrated market for euro-denominated retail payments and allows customers to make electronic payments to payees located anywhere in the SEPA area under the same basic terms and conditions. The principal EU legislation covering SEPA is Regulation (EU) No. 260/2012 (the "SEPA Regulation"). The description of the SEPA Regulation in its title is instructive; a regulation "*establishing technical and business requirements for credit transfers and direct debits in euro*".

The SEPA Regulation applies an equal charging principle for cross-border and national payments in euro to all transactions. SEPA does not cover payments via debit or credit cards or payments via mobile phone or other means of telecommunication or digital or IT devices (Recital 6). It merely applies to credit transfers and direct debits. SEPA establishes a technical platform so that a payment service provider which provides domestic credit and debit payment transactions, may provide those services on a European Union-wide basis and it ensures that payment schemes are inter-operable.

Article 3 of the SEPA Regulation, for example, requires that accounts be 'reachable' for credit transfers or direct debits initiated by a payer in another member state in accordance with relevant European rules. The system operates through the use of IBANs which provide identification requirements for EU payment service providers. SEPA encompasses a SEPA Credit Transfer Scheme and a SEPA Direct Debit Scheme, each of which is subject to a Rulebook that sets out the applicable rules for participation. There is no suggestion that the Provider in the present case, is in breach of the rules of either scheme.

Article 4(1)(a) of SEPA Regulation provides as follows:

> ***"Interoperability***
> 1. *Payment schemes to be used by [payment service providers] for the purposes of carrying out credit transfers and direct debits shall comply with the following conditions:*
>
> *(a) their rules are the same for national and cross-border credit transfer transactions within the Union and similarly for national and cross-border direct debit transactions within the Union*".

Article 4(2) mandates that each payment system is technically interoperable with other retail payment systems within the Union through the use of standards developed by international or European standardisation bodies. It directs that no business rules that restrict interoperability with other retail payment systems within the Union be utilised. Article 4(3) provides that the processing of credit transfers and direct debits shall not be hindered by technical obstacles.

'Payment system' is defined in Article 2 as "*a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing or settlement of payment transactions*". The definition makes no reference to security arrangements that can be applied to the processing of customer instructions. In fact Article 5(3) confirms that a payment service provider must ensure that the payer gives consent for a relevant payment.

/Cont'd…

In light of the terms of the SEPA Regulation, its purpose and application, I am not prepared to uphold the complaint that the Provider was not, or is not, entitled to require the use of the security device at issue for some but not all of it credit transfers pursuant to the SEPA Regulation.

Security arrangements may be more relevant to European regulations concerning payment services. The European Communities (Payment Services) Regulations 2009 (S.I. No. 383 of 2009) were in force at the time of the complaint. These have now been replaced by European Union (Payment Services) Regulations 2018 (S.I. No. 6 of 2018). A payment transaction is authorised by a payer only when the payer has given consent to execute the payment transaction. Consent is given in the form agreed between the payer and payment service provider concerned, such as to the input of a personal identification number. Payment service users are obliged to use payment instruments in accordance with the terms governing their use and issue.

The terms of the agreement between the Provider and the Complainant in this instance are set out in the terms and conditions relating to current accounts, including the student plus account at issue. Condition 5.5 provides as follows:

> *"You must authorise a transaction by:*
> *. . .*
> *5.5.2 following whatever instructions we may give to you or your authorised signatory authorised user in relation to the operation of your account by . . . our Internet banking service . . . and by such other Channels as we make available from time to time."*

The applicable terms and conditions for Internet banking dated May 2015 provides as follows:

> *"5.2 You authorise us to act on any instruction to debit an account received through [Internet banking] which has been transmitted using all or part of any security device and/or other authentication process (which may, or may not, include use of or part of a security device) which we may require to be used in connection with [Internet banking] without requiring us to make any further authentication or enquiry, and all such debits shall constitute a liability of you.*
>
> *. . .*
>
> *5.5. We may refuse to execute a transaction if:*
> *5.5.1 you have not authorised the transaction in accordance with Condition 5.2"*

By opening the relevant account with the Provider and agreeing to the relevant terms and conditions, the Complainant was therefore agreeing to comply with the security measures and authentication processes required of him by the Provider in relation to the processing of individual transactions. This is in accordance with the provisions of the Payment Services Regulations. There is no suggestion that any relevant term or condition of the Complainant's contract with the Provider has been breached. Rather, the Complainant argues that the

/Cont'd…

requirement for the security measure at issue is in breach of the SEPA Regulation on the basis that a different authorisation requirement applies to transactions up to a certain threshold where this transaction concerns domestic transactions rather than inter-EU transactions. As set out above, I do not accept that this constitutes a breach of the SEPA Regulations nor do I consider there to be any breach of the Payment Services Regulations in this regard.

It is of course always open to the Complainant to close his account with the Provider concerned and to open an account with another Provider which does not mandate the same security measure as has been implemented by the Provider, in its commercial discretion.

In all of the circumstances, I do not consider it appropriate to uphold the present complaint as the evidence, in my opinion, discloses no wrongdoing on its part.

/Cont'd…

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
DIRECTOR OF INVESTIGATION, ADJUDICATION
AND LEGAL SERVICES

31 August 2018

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.