Consultation: Proposed Amendments to Open Banking Regulations

Industry Comments and Feedback
July 2021

General Comments:		
Comments	**REF**	**CBB Response**
A licensee • Data shared with TPP/ancillary provider by the licensee should not be shared with unlicensed TPP and should not be used for secondary purposes. • It is unclear what the definition of Customer is. Shall we continue to consider it as a natural person, or will they include corporate customers?	GR1	The Open Banking regulations require that the account holding entities (currently, retail banks) share the data with TPPs who are subject to relevant rules under CBB Rulebook, Volume 5. The Module AU and Module OB of Volume 5 specify the scope of the services of TPPs and what they may do with customer data obtained, subject to also meeting the requirements of PDPL. Customers include both natural and corporate customers.
A licensee Taking note of the added points in LR-1.3.1 as part of the Regulated Banking Services for Vol 2 Licensees. **(o) Providing account information services; and** **(p) Providing payment initiation services.** Reading this point in addition to the definition in **LR-1.3.58**, does this mean that the bank can act as an aggregator without the need of involving a third-party? If so, who will be responsible to ensure that data does not get intercepted or saved at the participating licensees i.e. if Bank A is aggregating accounts for a customer (from Bank A, B and C) in its own Channel (e.g. Mobile Application), where should the data reside/flow? And what measures are expected to ensure that the participating bank's data (For Bank B and C in this example) is not intercepted or further analyzed / acted upon by Bank A?	GR2	Under the amended rules, retail banks can no longer "white-label" acting as agents of a licensed TPP, and those wishing to provide open banking services to customers must apply for CBB approval as per the amended requirements. The banks need to also comply with all the requirements of Module OB. A bank acting as aggregator will have access, with customer consent, to data as specified in Paragraph OB-1.1.13. With regards to where such data should reside, it would be dependent on the business model, the relevant use-cases, the Bahrain Open Banking Framework and the specific rules under Module OB.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
Volume 1 GR-6.1 Access to PISPs and AISPs	**A licensee** Please clarify if this access is limited to actual accounts only and not savings tools and features as well.	SP1	As per guidance in Paragraph GR-6.1.5 banks are required to share customer account information and that which can be accessed by the customer in a digital form based on the consent received. This includes customer transaction data and also product and services data that banks are required to publicly disclose. Banks may also share other information about products and services not required by the rules with AISPs in order to generate new revenue or business under bilateral arrangements with AISPs.
Volume 1 GR-6.1.3 Conventional retail bank licensees must: (a) grant ancillary service providers of the types referred to in Paragraph AU-1.2.1 (f) and (g) of Rulebook Volume 5: Ancillary Service Providers Authorisation Module, access to customer	**A licensee** With regard to subparagraph (b): Would recommend that the criteria be unified across Bahrain and be uniformly applicable to all banks and AISPs/PISPs.	SP2	The BOBF establishes the uniform technical specifications, customer experience requirements, operational guidelines and security standards for such access.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
accounts on an objective, non-discriminatory basis based on consents obtained from the customer; (b) provide the criteria that the conventional retail bank licensees apply when considering requests pursuant to sub-paragraph (a) above for such access; and (c) ensure that those criteria are applied in a manner which ensures compliance with sub-paragraph (a) above while ensuring adherence to Law No 30 of 2018, Personal Data Protection Law (PDPL) issued on 12 July 2018.			
Volume 1 GR-6.1.5 Access to customer accounts granted pursuant to Paragraph GR-6.1.3 shall mean that at customer's direction, the licensees are obliged to share, without charging a fee, all information, that has been provided to them by the customer and that which can be accessed by the customer in a digital form. The obligation should only apply where the licensee keeps that information in a digital form. Furthermore, the obligation should not apply to information supporting	**A licensee** While AISP/PISPs are allowed to charge a fee to their customers, however, the same is not true for the banks. Some fee sharing with AISP/PISPs should be allowed for since banks have invested in availing the OB infrastructure. To clarify: this is not applicable to payment instructions initiated by the customer through a PISP, in which	SP3	Disagree, it is important that information access specified in Module GR to AISPs/PISPs is free of charge to allow open banking adoption. Banks may leverage AISPs by ensuring they become a channel for new customers as in other aggregator models.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
identity verification assessment; which the licensees should only be obliged to share with the customer directly, not a data recipient. The information accessed shall include transaction data and product and services data that banks are required to publicly disclose, such as price, fees, and other charges should be made publicly available under open banking. Fees may be charged by banks to AISPs for sharing 'Value Added Data' and 'Aggregated Data'. Value added data or derived data results from material enhancement by the application of insights, analysis, or transformation on customer data by the licensee. Aggregated data refers to data which is aggregated across the licensee's customer segments for the purpose of analysis.	case, the bank's published charges will be applicable. The guideline states: The obligation should only apply where the licensee keeps that information in a digital form. Would suggest to add the following "and is accessible to the bank's customers through the bank's current digital channels"		Paragraph GR-6.1.5 has reference to "all information which can be accessed by the customer in a digital form".
	A licensee For value added services, is there a cap on fees and charges by CBB or do the bank's need to devise their own schedule for AISP's and PISP's? Are we obliged to provide value added services or is this optional?	SP4	Value added services are optional and the fees and charges should be based on bilateral arrangements between banks and AISPs/PISPs. Value added services are encouraged since this is where the true value of open banking lies. Moreover, such value-added services can help enhance revenues for banks and for TPPs.
<u>Volume 1</u> GR-6.1.7 Conventional retail bank licensees must comply with each of the following requirements: (a) provide access to the same information from designated customer accounts made available to the customer when directly requesting access to	**A licensee** The regulation requires AISP/PISP to be provided with a confirmation whether the amount necessary for the execution of a payment transaction is available as a "yes"/"no". For facilitating modern use cases like	SP5	The said requirement only applies to PISPs only as they should not have access to customer account balances. The sub-paragraph GR-6.1.7 (c) will be amended as follows: (c) upon request, immediately provide ~~AISPs and~~ PISPs with a confirmation whether the amount necessary for the

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
the account information, provided that this information does not include sensitive payment data (such as customer security credentials or other personalised data, the holding of which or the use of which is not authorised by the customer; and data which may be used by the holder for unauthorised, fraudulent, illegal or activity or transactions); (b) provide, immediately after receipt of the payment order, the same information on the initiation and execution of the payment transaction provided or made available to the customer when the transaction is initiated directly by the latter; (c) upon request, immediately provide AISPs and PISPs with a confirmation whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer. This confirmation must consist of a simple 'yes' or 'no' answer.	wallets, ecommerce payments - it is also required to make the balance available as part of the response to improve user experience to select the right payment account when multiple payment accounts have been setup. This is highly recommended to be incorporated in the regulations.		execution of a payment transaction is available on the payment account of the payer. This confirmation must consist of a simple 'yes' or 'no' answer.
Volume 1 GR-6.1.8 For the purposes of Paragraph GR-6.1.7, conventional retail bank licensees must	**A licensee**	SP6	In case of accounts belonging to legal entity, access should only be provided if a separate consent is received from that entity.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
provide access to information and data pertaining to customer account activity and balances covering a period of 12 full months or 365 days at the time of access to the AISPs in respect of the following services/products offered by the licensee: (a) Savings accounts; (b) Current accounts; (c) Term and call deposits; (d) Foreign currency accounts; (e) Unrestricted investment accounts; (f) Restricted investment accounts; (g) Mortgage/housing finance products; (h) Auto loans; (i) Consumer loans/financing; (j) Overdrafts (personal); (k) Credit and charge cards; (l) Electronic wallets and prepaid cards; and (m) Other accounts which are accessible to the customer through e-banking portal or mobile device.	With regard to subparagraph (m): The regulation must not be applicable for Legal Entity accounts. Justification: If a user is able to access both his/her personal account and company accounts (in which he/she is user, approver) through same portal, Bank's shall not be obliged to provide access to the legal entity account, as it generally requires the need for an explicit consent as per the legal entity mandate.		
	A licensee Unclear whether all data requests must be addressed for exactly 12 months as opposed to the earlier understanding of up to 12 months based on customer preference.	SP7	Up to 12 months refers to customer consent i.e. for how long an AISP can access customer information. This rule has reference to the data available to the customer at a particular point in time of access of his/her accounts. Data provided to AISP after obtaining customer consent must be for a historical period of 12 full months by default. However, customers can always choose a shorter period if the AISP gives an option to the customer.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
Volume 1 GR-6.3.12 Conventional retail bank licensees, AISPs, and PISPs, must have in place a strong customer authentication process and ensure the following: (a) no information on any of the elements of the strong customer authentication can be derived from the disclosure of the authentication code; (b) it is not possible to generate a new authentication code based on the knowledge of any other code previously generated; and (c) the authentication code cannot be forged.	**A licensee** The strong customer authentication process is undertaken by the licensees maintaining customer accounts and not the AISP / PISP. The clause should be amended to remove 'AISP/PISP' from volume 1 and 2 modules.	SP8	Agreed the amendment will be made: GR-6.3.12 Conventional retail bank licensees~~, AISPs, and PISPs,~~ must have in place a strong customer authentication process and ensure the following: (a) no information on any of the elements of the strong customer authentication can be derived from the disclosure of the authentication code; (b) it is not possible to generate a new authentication code based on the knowledge of any other code previously generated; and (c) the authentication code cannot be forged.
Volume 1 GR-6.3.13 Conventional retail bank licensees, must adopt security measures that meet the following requirements for payment transactions: (a) the authentication code generated must be specific to the amount of the payment transaction	**A licensee** Subparagraph (C) The requirement of SMS is applicable on TPP for customer access / initiate transaction to the Open Banking Application or Portal. For Open Banking, the customer access and	SP9	Banks are required to send payment transaction related SMSs when the account is accessed or when a transaction is initiated as per current practice. The obligation for SMS is on banks and not on TPP.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
and the payee agreed to by the payer when initiating the transaction; (b) the authentication code accepted by the licensee maintaining customer account corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer; (c) a SMS message must be sent to the customer upon accessing the online portal or application and when a transaction is initiated; and (d) any change to the amount or the payee must result in the invalidation of the authentication code generated.	initiate the transaction is through OB portal and accordingly requirement of sending SMS should not be on Bank. For the bank we currently send all mandatory SMS required under EFTS for transactions, irrespective of channel such request is received from customer. We request CBB clarification for this requirement is it on the Bank or on TPP, to send SMS message on accessing the online portal or application and when a transaction is initiated.		
Volume 1 GR-6.4.1 Conventional retail bank licensees must adhere to the Operational Guidelines, Security Standards and Guidelines, Open Banking Application Program Interface (API) Specifications and Customer Journey Guidelines included in Bahrain Open Banking Framework (see CBB website).	**A licensee** GR-6.4.1 & GR-6.4.2 Will this be still applicable if we do not have our own OB application and OB services are offered to our customers through the Gateway.	SP10	Yes, the bank is required to obtain CBB's written approval and is responsible for all the AISP/PISP services it provides to customers. The Gateway will only be an "outsourced technology provider" for this purpose. The bank is thus obliged to comply with Module OB of Volume 5.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
Volume 1 GR-6.4.2 Conventional retail bank licensees must ensure that compliance with standards and guidelines specified in Paragraph GR-6.4.1 is subject to independent review and tests, including testing in a test environment., by an independent consultant upon implementation.	**A licensee** Will CBB be providing the names of organizations in Bahrain who would be certified to conduct these independent reviews? Is the independent review required to be performed as a one-off exercise or is it required to be conducted upon major implementations?	SP11	No, but the banks can enquire if a particular consultant is acceptable to the CBB by contacting their SPOC. Currently, it is only applicable upon implementation.
Volume 1 LR-1.3.1B A conventional bank licensee that wishes to undertake regulated banking services which were not included in its application for licence must obtain CBB's written approval prior to offering such services. In such situations, CBB may impose additional conditions that it deems necessary for the provision of such services.	**A licensee** Does this effect the current service (Aggregator)? Even though this service is offered by a Gateway (Licensed AISP) and it is been integrated in the bank's App.	SP12	See SP10
Volume 1 LR-1.3.61 Conventional retail bank licensees that wish to offer AIS or PIS services must ensure that an independent review is conducted prior to commencement of AIS or PIS services to confirm compliance with the Operational Guidelines,	**A licensee** Will CBB be providing the names of organizations in Bahrain who would be certified to conduct these independent reviews?	SP13	See SP11

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
Security Standards and Guidelines, Open Banking Application Program Interface (API) Specifications and Customer Journey Guidelines included in the Bahrain Open Banking Framework available on the CBB website. Such a review must be conducted by a third-party consultant, other than the external auditor.			
Volume 1 BR-4A.6.1 Conventional retail bank licensees must report to CBB statistics on the availability and performance of APIs on a monthly basis as per the requirements included in the Operational Guidelines in the Bahrain Open Banking Framework. The reports must be submitted within 5 working days of the month end.	**A licensee** We suggest CBB assume 100% uptime, if any bank has any downtime then a report should be sent to CBB as per CBB instructions.	SP14	The reporting requirement includes statistics besides uptime.
	A licensee We seek clarification on the mechanism to be followed for the report sharing, is there going to be a specific portal to upload this report, or	SP15	The SPOC in the FMIs and Payment Oversight Division will provide guidance to licensees.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
	we are expected to share it by Email or any other method.		
Volume5 GR-12.1.3 All licensees must perform penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place at least twice a year. These tests must be conducted each year in June and December simulating real world cyber attacks on the technology environment and must: (a) Follow a risk-based approach based on an internationally recognised methodology, such as National Institute of Standards and Technology "NIST" and Open Web Application Security Project "OWASP"; (b) Include both Grey Box and Black Box testing in its scope; (c) Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services; (d) Be performed by external, independent third parties which must be changed at least every two years; and	**A licensee** We request that the penetration testing be reduced to at least once a year from the proposed two times.	SP16	Bi-annual testing is required due to cyber security risks faced by licensees offering digital financial services.
	A licensee We thank CBB for considering and amending the GR-12 Security measures/Cybersecurity section. However, we feel the information provided here is not very detailed like how it is documented in UK open banking standards. https://www.openbanking.org.uk/wp-content/uploads/Participant-Guide-Information-Security-Operations.pdf	SP17	This section only refers to the penetrating testing requirement. Specific open banking security requirements are included in OB Module and the security guidelines of Bahrain Open Banking Framework.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
(e) Be performed on either the production environment or on nonproduction exact replicas of the production environment.			
Volume5 GR-12.2.4 Reports on penetration testing referred to in Paragraph GR-12.1.3 must be submitted to CBB before 31st August for the tests as at 30th June and 28th February for the tests as at 31st December. The penetration testing reports must include the vulnerabilities identified and a full list of 'passed' tests and 'failed' tests together with the steps taken to mitigate the risks identified.	**A licensee** We request that the timeframe for submitting any penetration testing reports be increased to at least three months from the proposed two months.	SP18	Agreed. The rule will be amended as follows: GR-12.2.4: Reports on penetration testing referred to in Paragraph GR-12.2.3 must be submitted to CBB before 30th September for the tests as at 30th June and 31st March for the tests as at 31st December. The penetration testing reports must include the vulnerabilities identified and a full list of 'passed' tests and 'failed' tests together with the steps taken to mitigate the risks identified.
Volume 5 AU-4.7.9 AISPs/PISPs must submit a report of an independent review undertaken by a third party expert confirming compliance with the Bahrain Open Banking Framework prior to going live. The detailed scope and procedures for such review and the appointment of the third party expert must be approved by CBB.	**A licensee** Further details about the reports, accessibility and third party approved providers that performs the same.	SP19	As mentioned in the rules, the CBB will approve the scope of the review and the third party expert upon application. Any further details can be obtained at that stage.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
Volume 5 OB-1.1.4 The internal controls must include, but not be limited to, those relating to the following: (a) The development and or acquisition of the technology solutions to conduct the activity; (b) Testing of the solutions and application program interfaces; (c) Standards of communication and access and security of communication sessions; (d) Safe authentication of the users; (e) Processes and measures that protect customer data confidentiality and personalised security credentials consistent with Law No. 30 of 2018, Personal Data Protection Law (PDPL) issued on 12 July 2018; (f) Tools and measures to prevent frauds and errors; (g) Security policy; (h) Information security testing including web applications testing, configuration reviews, penetration testing and smart device application testing (i) Risk management controls;	**A licensee** We also observed that there have been no proposed updates made to the below clause which was earlier clarified to the CBB. 'The internal controls must include, but not be limited to, those relating to the following: (j) Prevention of anti-money laundering (AML) and combating terrorist financing (CTF);' KYC on customers is undertaken by the licensees maintaining customer accounts and not by the AISP/PISP. AML/CFT controls are to be implemented by the ASPSPs. Please amend the clause accordingly.	SP20	Ancillary services providers are required to comply with Module FC of Volume 5 of the CBB Rulebook. ASPSPs are subject to Module FC requirements of Volumes 1 or 2 as appropriate.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
(j) Prevention of anti-money laundering (AML) and combating terrorist financing (CTF); (k) Record keeping and audit trails; and (l) Operational and financial controls.			
Volume 5 OB-1.1.12 A PISP must establish procedures to ensure: (a) that it will not store a customer's personalised security credentials, such as customer's KYC and biometric information and that such data are: i. not accessible to other parties, with the exception of the issuer of the credentials; and ii. transmitted through safe and efficient channels; (b) that any other information about a customer is not provided to any person except a payee, and is provided to the payee only with the customer's explicit consent;	**A licensee** With regard to subparagraph (b): We feel the use of term "Other information" may include some personal information about customer which still identifies the customer. So security of Payee system must be enforced. The "explicit consent" process is not detailed with "where, when and what PISP should show to customer on behalf of payee" anywhere.	SP21	The rules require prior customer consent for any other information (including customer identifying information) to be provided to payee. The payee details are provided by the customer (payer) so such details are not required.
(c) that each time a PISP initiates a payment order on behalf of its customer, the PISP identifies itself to the PISP, the licensee with whom he the customer maintains the account in a secure way; (e) that it will not access, use or store any information for any purpose except for the	**A licensee** OB-1.1.12(b) The regulation requires that information must not be provided to any person except a payee. In certain instances, some payment information	SP22	OB-1.1.12 (b) refers to other information i.e. information in addition to the necessary payment details to execute the transaction. Any such information should only be given to the payee. Also, none of the situations mentioned in the comments provided will fall under (b).

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
provision of a payment initiation service explicitly requested by a payer, however, it may store payment details initiated by the customer such as payment amounts, payment accounts, payment reference number, payment execution dates, time and payee's IBAN number; (f) that it cannot and does not change the amount, the payee or any other feature of a transaction notified to it by the customer; and (g) that any data accessed and stored is encrypted in transit and at rest and, must not be accessible to any unauthorised person within the licensee's organisation.	related to a customer needs to be shared with clients which may not necessary be the Payee but could be an institution or a service that offers payments i.e., digital wallet funding, digital account opening, SMB payments to suppliers, etc. The clause should be amended accordingly to allow the above.		
<u>Volume 5</u> OB-1.1.13 An AISP must establish account information procedures to ensure: (a) it does not provide account information services without the customer's explicit consent;	**A licensee** Shouldn't the AISP provide a confirmation to the customer that all data stored with the AISP has been deleted when consent is revoked?	SP23	As specified in Sub-paragraph (g) must not be stored in a form which permits identification of customer once the customer consent is withdrawn.
(b) that it will not store the customer's personalised security credentials such as	**A licensee** With regard to subparagraph (f): The information which are generated by	SP24	Sub-paragraph (g) addresses these points adequately.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
customer's KYC and biometric information and that such data are: i. not accessible to other parties, with the exception of the issuer of the credentials; and ii. transmitted through safe and efficient channels; (c) for each communication session, communicate securely with licensee and the customer in accordance with the regulatory requirements of this Module; (d) that it does not access any information other than information from designated accounts; (e) it will not access, use, or store any information for any purpose except for the provision of the account information service explicitly requested by the customer; (f) that any data accessed and stored is encrypted in transit and at rest and, must not be accessible to any unauthorised person within the licensee's organisation; and (g) that customer information accessed must not be stored in a form which permits identification	AISP/PISP by running algorithms and data analytics systems must remove any information which identifies the customer after the data analytics processing is done. With regard to subparagraph (g): We feel Customer Device fingerprints generated by the AISP/PISP system when user was accessing the system must be protected and device traces must be anonymized.		
	A licensee OB- 1.1.12(a) & OB-1.1.13(b) AISP/PISPs offer their products to multiple merchant/bill payments enabling consumers to make payments using bank accounts. To improve the consumer / user payment journey, as well as authentication experience, TPPs need to have access and store certain customer information like CPR, Phone #, email. The clause should be amended / clarified accordingly to allow the above.	SP25	The use case mentioned is allowed under the current rules and the customer experience guidelines in BOBF must be followed.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
of customer once the customer consent is withdrawn.	OB-1.1.13(d) "that it does not access any information other than information from designated accounts; "AISPs are limited to and are only able to access data provided / granted by licensees maintaining customer accounts based on customer consent. This requirement should be included in the retail banking modules (volume 1 & 2) as ASPSP are the ones who have control on the information to be shared. OB-1.1.13(g) This regulation requires data to be stored in an anonymized manner post customer consent withdrawal. We recommend including a time period (in line with the CBB / PDPL record retention requirements) post withdrawal - from the following perspectives: · Internal / external auditors require data, as appropriate. · From a customer support perspective		This requirement is additional safeguard for customer data protection. Details such as identity of the customer and his history with the AISP i.e. what services he used and during which period can be kept for auditing or for other purposes; however, account information and account transaction history would need to be anonymized or deleted.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
	wherein any queries / concerns that need to be addressed post withdrawal of the consent would require data to be identifiable.		
Volume 5 OB-2.2.1 AISPs and PISPs must have in place a strong customer authentication process and ensure the following: (a) no information on any of the elements of the strong customer authentication can be derived from the disclosure of the authentication code; (b) it is not possible to generate a new authentication code based on the knowledge of any other code previously generated; and (c) the authentication code cannot be forged.	**A licensee** The strong customer authentication process is undertaken by the licensees maintaining customer accounts (ASPSP) and not the AISP / PISP. This clause should be removed from this module and be part of volume 1 & 2 (GR-6.3.12).	SP26	Agreed, the paragraph will be amended to simply require good user access security as follows: OB-2.2.1 "AISPs and PISPs must have in place a 2 factor authentication process to prevent unauthorised access."
Volume 5 OB-2.3.7 PISPs must ensure that a customer to whom a payment instrument has been issued must keep safe the personalised security credentials and must: (a) use it in accordance with the terms and conditions governing such use; and	**A licensee** OB-2.3.7(b) The wordings in the regulation require the customer to whom a payment instrument has been issued to ensure (a) and (b). The way the requirement is worded seems as if the PISP needs to	SP27	The requirement is for PISPs to ensure that their customers abide by (a) and (b).

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB Response**
(b) notify the PISP in an agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.	notify the PISP. The clause needs to be eased for appropriate interpretation.		