PSD2 CONTINGENCY EXEMPTION FORM – ILLUSTRATIVE ANSWERS*

The answers in this document have been compiled by UK Finance and the Open Banking Implementation Entity (OBIE) and every effort has been made to align to the existing regulatory requirements and the FCA Approach Document. They are illustrative and intended to provide examples for firms on how their implementation of API standards meet PSD2 requirements.

When completing the form, firms must ensure that their answers accurately reflect the interface and processes that they have implemented and the particular circumstances of the firm.

The FCA has commented on an earlier version of this form – but this is not FCA guidance. Completing the form along the lines of the illustrative answers will not guarantee that the FCA will grant an exemption. In considering a firm's answers, the FCA may also ask for further information.

Firms are free to choose how they create a dedicated interface, and can approach the completion of the form in different ways and with different answers.

Where relevant, reference to the OBIE Standard (API Specifications, Security Profile, Customer Experience Guidelines "CEG" and Operational Guidelines "OG") has been made to assist those firms participating in the Open Banking ecosystem. It should be understood that these are intended to provide additional guidance and abiding by the OBIE Standard principles can be used to assist a firm's application for an exemption.

*ASPSPs should submit final answers via the FCA Connect portal using the FCA's published form.

The FCA's exemption team can be contacted at PSD2-CER@fca.org.uk. See the FCA's contingency exemption webpage for more information.

Guidance on the information to be provided can be found in the FCA's Payment Services and Electronic Money Approach Document, section 17.102.

Version 1.0
Publication date: 5 April 2019

FORM A

Ref	Question	Points to note and illustrative examples
D1	Financial Registration Number (FRN):	FRN: XXXXXX
D2	Interface Name/Id (ASPSPs submitting a return should provide the name or ID used within the PSP to identify the interface being reported on)	**Points to note for this answer:** • If an ASPSP has multiple dedicated interfaces, a unique name should be given to each interface to prevent confusion about which dedicated interface is the subject of the exemption request. **Illustrative example:** “Example Bank corporate dedicated interface”
D3	If this is a single request for a dedicated interface operated across different banking brands, subsidiaries or products, please provide the names of the different banking brands, subsidiaries or products	**Illustrative example:** “Yes” “The dedicated interface enables access to accounts provided under the following brands which are part of the and products [Example Bank Group]: • Example Bank Brand 1 – Retail banking • Example Bank Brand 1 – Commercial banking • Example Bank Brand 2 – Commercial banking • Example Bank Brand 2 – Private wealth
D4	If this is a request for one of a number of dedicated interfaces being operated across different banking brands, subsidiaries or products, please identify the group (e.g. banking group) and the brand, subsidiary or product which is the subject of this request	**Illustrative example:** “Yes” This exemption request covers Example Bank Brand 1’s commercial banking dedicated interface only”

Ref	Question	Points to note and illustrative examples
D5-8	Contact details of the person we will get in touch with about this application	**Name**: Jane Smith **Role within organisation:** Head of PSD2 Delivery **Telephone number:** 090900908 **Email address:** Jane.smith@examplebank.com
Q1	Has the ASPSP defined service level targets for out of hours support, monitoring, contingency plans and maintenance for its dedicated interface that are at least as stringent as those for the interface(s) used by its own payment service users (EBA Guideline 2.1)?	**Points to note for this answer:** • Answer should be **yes** to meet exemption criteria. • See FCA guidance at AD 17.113. • See EBA Guideline 2. • See OBIE Operational Guidelines Chapters 4, 5 and 6. • Supporting information can be provided (a box has been added to the form to accommodate this) and should include an explanation that out of hours support, monitoring, contingency plans and maintenance for the dedicated interface, provided for the dedicated interface are equivalent to those provided for the customer interface. **Illustrative answer:** • There is a dedicated support team for the dedicated interface (as there is for customer online banking). • The support team can be contacted by TPPs to provide technical support 24/7 (which is the same level of support we provide to online banking customers). • There is real time monitoring of both the dedicated interface and customer online banking, which provides alerts to the support team if there are outages or other problems. • We have contingency plans for both customer online banking and the dedicated interface which set out possible scenarios which may impact continuity of service and how to restore service. • Maintenance of both the dedicated interface and customer online banking is undertaken during our non-prime time (X time – Y time), we undertake maintenance on the customer interface in the same non-prime hours. Other answers may be given.
Q2	Has the ASPSP put in place measures to calculate and record performance and availability indicators?	**Points to note for this answer:** • Answer should be **yes** to meet exemption criteria. • See FCA guidance at AD 17.113. • See EBA Guideline 2. • See OBIE Operational Guidelines, Section 2.1, Key indicators for availability and performance, which provides detailed guidance on how availability and performance can be calculated. • No supporting information is required, but ASPSPs should note the requirement for calculating performance and availability in EBA Guideline 2.

Ref	Question	Points to note and illustrative examples
		• From 14 September 2019, ASPSPs will need to publish this data on their websites quarterly and also report the data to the FCA quarterly using REP020.
Q3	Please set out the plan for the quarterly publication of daily statistics on the availability and performance of the dedicated interface and payment service user interface.	**Points to note for this answer:** • See FCA guidance at AD 17.114. • See EBA Guideline 3. • See OBIE Operational Guidelines, Section 2.2, Publication of statistics. **Illustrative answer:** • Our publication of statistics each quarter will present daily availability and performance statistics (measured and calculated as per EBA Guideline 2). • We will publish statistics for each previous quarter on: ○ X January (Q4) ○ X April (Q1) ○ X July (Q2) ○ X October (Q3) • We will publish statistics from X date – Y date on Z date. • The statistics will be published in close proximity to (and will be accessible via) our service availability dashboard (required under BCOBS 7) – URL XXXXX • We will publish a line chart to enable a comparison between the performance and availability of the dedicated interface and the performance and availability of the user interface. Other answers may be given.
Q4	Please provide a summary of the results of stress tests undertaken.	**Points to note for this answer:** • See FCA guidance at AD 17.118. • See EBA Guideline 4. • See OBIE Operational Guidelines Chapter 3. • The answer should cover: ○ The results of the stress testing. ○ The assumptions used as a basis for stress testing. ○ How any issues identified during stress testing have been addressed. • EBA Guideline 4.2 a-d sets out the capabilities that should be tested as a minimum, these are: a) the capability to support access by multiple PISPs, AISPs and CBPIIs;

Ref	Question	Points to note and illustrative examples
		b) the capability to deal with an extremely high number of requests from PISPs, AISPs and CBPIIs, in a short period of time without failing; c) the use of an extremely high number of concurrent sessions open at the same time for payment initiation, account information and confirmation on the availability of funds requests; and d) requests for large volumes of data. **Illustrative answer:** We have designed our procedures to stress test the dedicated interface in line with EBA Guideline 4. We undertook stress testing between [X date] and [Y date]. Based on this stress testing, we are confident that the performance and availability of the dedicated interface will not be adversely affected by peak usage of the interface by TPPs, or other stresses on the system. <u>Assumptions used</u> We did the following to forecast likely API request volumes: • Engaged with TPPs to understand the demand of their customers for access to our accounts • Analysed current demand for access to our accounts via screen scraping • Hypothesised what normal use would look like in year 1 (post September 2019) • Assessed what large volume data requests would look like <u>Testing</u> • We subjected the dedicated interface to the following scenarios to test the capabilities outlined in the EBA guidelines: [Insert scenarios] <u>Result:</u> The interface did not fail during this period of testing. [OR The interface failed during the first period of testing. We made changes to the interface and repeated the testing, after which the interface did not fail under the same conditions.] Other answers may be given.
Q5	Please describe the method(s) of carrying out the authentication procedure(s) of the payment service user that are supported by the dedicated interface.	
a	**Redirection** Summary of the authentication	**Redirection**

Ref	Question	Points to note and illustrative examples
	procedure	**Points to note for this answer:** • See FCA guidance at AD 17.122 -17.129. • See EBA Guideline 5. • See OBIE Customer Experience Guidelines section 2.2. • The ASPSP should give a description of the authentication procedure facilitated by its dedicated interface. • Detail of the authentication procedure can be given as an illustration provided as a separate attachment to the form, a brief summary should also be provided in the form. • ASPSPs can use this section to explain whether or not they have followed the OBIE customer experience guidelines as they relate to authentication procedures. **Illustrative answer:** <u>Summary of the authentication procedure</u> • Once consent has been given to the AISP or PISP to access a PSU's account, the PSU is redirected automatically to the ASPSP webpage or mobile app to provide authentication details. • The PSU is also redirected automatically to the ASPSP webpage or mobile app to provide authentication details, where the PSU provides us with their explicit consent for the provision confirmation of funds responses for each specific CBPII, prior to the first request. • We provide the same of authentication method(s)/ procedure(s) for TPP services, as those which are available to the PSU when accessing our direct channels. Accordingly, we support web-to-web and app-to-app redirection for this purpose. Specifically, for accounts and PSUs who have installed and use our mobile banking app, and where the PSU is using a TPP app on their mobile device, the PSU is redirected to authenticate with the mobile banking app without any additional web pages or screens. We also support the use of biometric authentication. • Once the PSU authenticates, they are redirected back to the AISP/PISP/CBPII domain for the completion of the process. • We have also decided to enable web-to–app authentication as described in our decoupled answer at 5(c) below. Other answers may be given.
b	Explanation of why the methods of carrying out the authentication procedure does not create	**Points to note for this answer:** • See FCA guidance at AD 17.130 – 17.150. • See OBIE Customer Experience Guidelines, section 2.0.

Ref	Question	Points to note and illustrative examples
	obstacles	The ASPSP should use this answer to provide evidence that the dedicated interface does not give rise to unnecessary delay, friction or any other attributes that would mean that customers are directly or indirectly dissuaded from using the services of PISPs, AISPs and CBPIIs. Please consider the following types of obstacles and provide an explanation, where applicable: **(i) Authentication Methods:** *If relevant* - an explanation if authentication methods that the customer can use when directly accessing their account are not available to the customer when accessing their payment account through an AISP or using a PISP. **(ii) Additional Authorisation/ Registrations:** *If relevant* - an explanation of any additional authorisation or registration steps imposed on AISPs, PISPs or CBPIIs, or any API enrolment steps, and a description of what those steps entail and why those steps do not impose obstacles **(iii) Additional Checks on consent:** *If relevant* - an explanation of any additional checks on the "explicit consent" given by the PSU to the AISP or PISP *If relevant*- an explanation of any additional checks on the "explicit consent" given by the PSU to the CBPII (pursuant to PSD2, Article 65(2)(a)) **(iv) More than one SCA per customer journey** *If relevant* - an explanation of why SCA is requested more than once per single session of AIS/PIS *If relevant* - an explanation why SCA is requested more than once in a CBPII session for provision of "explicit consent" to us prior to the first request (pursuant to PSD2, Article 65 (1)(b) and(c)) **(v) Superfluous or additional steps or language in the customer journey** *If relevant* - an explanation of any additional steps or language in the customer journey, and an explanation of why those steps do not impose obstacles • ASPSPs can also include the following: - Evidence concerning usage of the interface (e.g. successful calls on API) and customer drop-out rates. - Evidence of consumer testing or alignment to market initiative specifications that have had the input of

Ref	Question	Points to note and illustrative examples
		consumers **Illustrative answer:** We have implemented our redirection process in a way that is not an obstacle for AISPs and PISPs, as referred to in Article 32(3) of the SCA- RTS, to provide services to their customers. We confirm that our dedicated interface does not give rise to unnecessary delay or friction in the experience available to the PSUs when accessing their account via a PISP, AISP or CBPII or to any other attributes, including unnecessary or superfluous steps or the use of unclear or discouraging language, that would directly or indirectly dissuade the PSUs from using the services of PISPs, AISPs and CBPIIs. For each AISP, PISP and CBPII user journey, we have followed the Open Banking Customer Experience Guidelines v1.2 without deviation. In particular, we only require a single SCA step for each PSU journey as outlined below: • SCA is only requested once per single session/customer journey of AIS/PIS (unless an available exemption applies). • SCA is requested once in the single session where the PSU provides us with their explicit consent for the provision confirmation of funds responses for each specific CBPII, prior to the first request. • In relation to the proposed obstacle in point **(ii)**: We confirm AISPs, PISPs and CBPIIs are able to enrol onto the Open Banking Directory. TPPs can onboard automatically to the Open Banking Directory using just their eIDAS certificate (i.e. with no manual steps or obstacles) and then they can register each of their applications automatically with our dedicated interface using the Open Banking Dynamic Client Registration Specification (again with no manual steps or obstacles). In line with the FCA Approach Document, paragraph 17.140, we confirm that these completing these steps do not constitute an obstacle. • In relation to the proposed obstacle in point **(v)**: We confirm that we do not display any unnecessary or superfluous language, information or steps within our customer journeys. Other than the authentication step(s)/screen(s), the PSU will only be shown an additional screen in our website or mobile app, as outlined below: - We do allow for account selection, where the PSU has more than one account and the TPP has not provided the account details. - We only display supplementary information related to the payment, in circumstances when we would be required to display the same information to the PSU before a payment is made in our direct channel, for example, charges for international payments. • The customer is taken through [X] number of ASPSP screens before being sent back to the TPP. The customer is taken through [X] number of ASPSP screens in our direct channel for authentication.

Ref	Question	Points to note and illustrative examples
		- Customer testing shows these journeys take [X] seconds on average to complete and there is [X] % abandonment from when the PSU is redirected to our website or mobile app to when they are redirected back to the TPP. Other answers may be given.
c	**Decoupled** Summary of the authentication procedure	**Points to note for this answer:** - See FCA guidance at AD 17.127. - See OBIE Customer Experience Guidelines section 2.3 **Illustrative answer:** - Where a TPP redirects the PSU to our dedicated interface and has included the PSU's userID, and where we recognise that the PSU is an active mobile app customer, we send a push notification to the PSU's mobile device. - The PSU is then prompted to open their mobile banking app and authenticate. - Immediately after the PSU has authenticated, we return an access token to the TPP and the TPP can access the PSU's account. - We have implemented this for both AISP and PISP flows in line with the OBIE CEG v1.2, section 2.3.1. Other answers may be given.
d	Explanation of why the methods of carrying out the authentication procedure does not create obstacles	**Illustrative answer:** <u>Summary of the authentication procedure</u> This functionality allows our mobile-only PSUs to authenticate with their mobile banking app when accessing a TPP application on a desktop device. It enables the PSU to have access to a multitude of TPP services, without an authentication channel dependency. It provides the PSU with the flexibility to authenticate with the methods they are accustomed to, therefore supporting a wider range of TPP service offerings. Other answers may be given.
e	**Embedded** Summary of the authentication procedure	**Points to note for this answer:** - See FCA guidance at AD 17.128. - The OBIE Standard does not support embedded authentication.

Ref	Question	Points to note and illustrative examples
f	Explanation of why the methods of carrying out the authentication procedure does not create obstacles	n/a
Q6	Please provide information on whether, and, if so, how the ASPSP has engaged with AISPs, PISPs and CBPIIs in the design and testing of the dedicated interface.	**Points to note for this answer:** • See FCA guidance at AD 17.150 – 17.154 • See EBA Guideline 6 • See OBIE Operational Guidelines, chapter 3. **Illustrative answer:** We have implemented the OBIE Standard. This Standard has been developed over a period of 18 months in collaboration with nine of Europe's largest financial institutions as well as 500+ representatives from other ASPSPs, TPP communities, PSD2 and consumer stakeholder groups, and prominent fintech leaders. We have run OBIE Functional and Security Conformance Tools completed satisfactory passing for all mandatory tests, and self-attested to the Customer Experience Guidelines, which indicate conformance to the OBIE Standard. During the design and testing of our dedicated interface, we have created a developer portal to allow TPPs to access and register for access to our testing facility. This developer portal is accessible from our website's homepage. We have also run a series of hackathons and developer workshops to encourage TPPs to use our testing facility, and we have published links to our portal and various blog posts on these events on LinkedIn (see links) We have also engaged in the Open Banking Buddying Scheme, which paired us up with [X number] of AISPs, [X number] of PISPs, and [X number] of CBPIIs, who have helped us to test using our testing facility and engage in live proving of our dedicated interface. The transparency calendar provides an overview of our approach to a number of key delivery aspects of our interface. This is available here: https://openbanking.atlassian.net/wiki/spaces/AD/pages/996214149/Transparency+Calendar Other answers may be given.
Q7	Please provide the date from which the ASPSP has made available, at no charge, upon request, the documentation of the	**Points to note for this answer:** • See FCA guidance at AD 17.156 – 17.158. • See EBA Guideline 6.

Ref	Question	Points to note and illustrative examples
	technical specification of any of the interfaces specifying a set of routines, protocols, and tools needed by AISPs, PISPs and CBPIIs to interoperate with the systems of the ASPSP.	• The answer must be **14 March 2019** if an ASPSP is seeking to be exempt for 14 September 2019. • Alternatively, at least 6 months prior to the target date for the market launch of the dedicated interface* **If implementing this requirement after 14 March 2019 different timelines will apply.* Other answers may be given.
Q8	Please provide the date on which the ASPSP published a summary of the technical specification of the dedicated interface on its website and a web link.	**Points to note for this answer:** • See FCA guidance at AD 17.156 – 17.158. • See EBA Guideline 6. • The answer must be **14 March 2019** if an ASPSP is seeking to be exempt for 14 September 2019. • Alternatively, at least 6 months prior to the target date for the market launch of the dedicated interface*. ** If implementing this requirement after 14 March 2019 different timelines will apply.* Other answers may be given.
Q9	Please provide the date on which the testing facility became available for use by AISP, PISPs, CBPIIs (and those that have applied for the relevant authorisation. (dd/mm/yyyy)	**Points to note for this answer:** • See FCA guidance at AD 17.156 – 17.158. • See EBA Guideline 6. • The answer must be **14 March 2019** if an ASPSP is seeking to be exempt before for 14 September 2019. • Alternatively, at least 6 months prior to the target date for the market launch of the dedicated interface*. ** If implementing this requirement after 14 March 2019 different timelines will apply.* Other answers may be given.
Q10	Please provide the number of different PISPs, CBPIIs, AISPs that have used the testing facility.	**Illustrative answer:** Since 14 March 2019*, the following number of TPPs have used our testing facility: • [x number] PISPs • [x number] AISPs

Ref	Question	Points to note and illustrative examples
		- [x number] CBPIIs ** If implementing this requirement after 14 March 2019 different timelines will apply.* Other answers may be given.
Q11	Please provide a summary of the results of the testing.	**Points to note for this answer:** - See FCA guidance at AD 17.159 – 17.160. - See EBA Guideline 6. - See OBIE Operational Guidelines Section 3 and 6. - The answer should include: o a summary of the feedback received from PISPs, AISPs and CBPIIs. o a summary of any issues identified. o a description of how any problems or issues have been addressed. **Illustrative answer:** We have regularly engaged with the OBIE Service Desk since [x date]. We initially received feedback that there were problems with TPP onboarding, which we fixed by [x date] and, since then, all [x number] TPPs have successfully onboarded to our testing facility and have been able to run their own tests. We have received no reports of any issues from either AISPs or CBPIIs. However, we have received 2 reported issues from PISPs: - All [x number] PISPs reported that there was an additional step in our authentication for all payments where PSUs were asked to confirm the payment detail. This step has now been removed. Date reported: [x date], Date fixed: [x date]. - [x number] PISPs reported that there was an error with a minor delay relating to receipt of error messages. This has now been rectified. Date reported: [x date], Date fixed: [x date]. Other answers may be given.
Q12	Please provide a description of the usage of the dedicated interface in a three month (or longer) period prior to submission	**Points to note for this answer:** - See FCA guidance at AD 17.164 – 17.169 and AD 17.170. - See EBA Guideline 7. - OBIE Operational Guidelines, Section 3.3.

Ref	Question	Points to note and illustrative examples
	of the exemption request.	• If the production interface has been launched at different times for different products, provide a breakdown of when the access was available **Illustrative answer:** The three month period of wide use of the dedicated interface (live, production APIs for AIS, PIS and CBPII) ran from 14 March–14 June 2019. In that period, the number of PISPs, AISPs and CBPIIs that have used the interface to provide services to customers was: • [X number] of PISPs • [X number] of AISPs • [X number] of CBPIIs In that period, the number of separate requests sent by AISPs and CBPIIs to the ASPSP via the dedicated interface that have been replied to by the ASPSP: • PISPs = [X number of requests] • AISPs = [X number of requests] • CBPIIs= [X number of requests] *If relevant:* The production interface enabled AIS access: • To current accounts from X date • To credit cards from X dates • To payment enabled savings account from X date The production interface enabled PIS access: • To current accounts from X date • To payment enabled savings account from X date **Alternative illustrative answer:** We launched our dedicated interface (live, production APIs for AIS, PIS and CBPII) on 1 May 2019. We will provide an update to the statistics below on 1 August 2019 in order to demonstrate that we meet the criteria for exemption. Since 1 August 2019, the number of PISPs, AISPs and CBPIIs that have used the interface to provide services to customers

Ref	Question	Points to note and illustrative examples
		was: • [X number] of PISPs • [X number] of AISPs • [X number] of CBPIIs During that period, the number of separate requests sent by AISPs and CBPIIs to the ASPSP via the dedicated interface that have been replied to by the ASPSP are as follows: • PISPs = [X number of requests] • AISPs = [X number of requests] • CBPIIs= [X number of requests] Other answers may be given.
Q13	Describe the measures undertaken to ensure wide use of the dedicated interface by AISPs, PISPs, CBPIIs.	**Points to note for this answer:** • See FCA guidance at AD 17.169. • See EBA Guideline 7. **Illustrative answer:** Prior to launching the dedicated interface (production API for AIS, PIS and CBPII) we communicated the date from when it would be available, in the following ways: • On our website (at www.examplebank.com/APIdeveloper portal). • LinkedIn posts on [X date] and [Y date]. • Engagement with Open Banking Implementation Entity (including publication of various dates on their ASPSP calendar and regular communications via their Testing Working Group). • Engagement with FDATA, Fintech Scotland, and Electronic Money Association. • Roundtable on [X date]. • Engagement with [X number] of TPPs, comprising of [X number] of AISPs, [X number] of PISPs and [X number] of CBPIIs. Other answers may be given.
Q14	Please describe the systems or procedures in place for tracking,	**Points to note for this answer:**

Ref	Question	Points to note and illustrative examples
	resolving and closing problems, particularly those reported by AISPs, PISPs, and CBPIIs.	• See FCA guidance at AD 17.171. • See EBA Guideline 8. • See OBIE Operational Guidelines Chapters 4, 5 and 6. **Illustrative answer:** Frontline technical support for our dedicated interface is via our Service Desk provided for by [external company] who manage all tickets raised by TPPs as well as providing end user support to all our PSUs for our main customer interface and mobile banking apps. Where [external company] is unable to resolve the issue, this is raised to our 2nd line support staff within the bank. Should further support be required, our 3rd line support is formed of our interface development team who, in conjunction with our technical providers, resolve the problem to the best of their ability. When the problem is resolved, the TPP is informed and the ticket is closed. We also use the OBIE Service Desk to give TPPs an additional channel to report any issues. We have an automated process to keep all relevant tickets synchronised between both service desks. Other answers may be given.
Q15	Please explain any problems, particularly those reported by AISPs, PISPs and CBPIIs, that have not been resolved in accordance with the service level targets set out in EBA Guideline 2.1.	**Points to note for this answer:** • See FCA guidance at AD 17.171 and 17.172. • See EBA Guideline 8. • See OBIE Operational Guidelines Chapters 4, 5 and 6. • ASPSPs should include a description of problems reported during both testing and operational use ('production') of the dedicated interface. • The FCA will take into account, as part of its assessment, problems reported by AISPs, PISPs and CBPIIs. This answer should state the dates and times of incidents, the timelines to each resolution and the steps taken to resolve the problem(s). Below is an example of the expected level of detail. **Illustrative answer:** On [X date], we suffered a major outage due to a system failure with one of our technical service providers. This resulted in our customers being unable to utilise both PISP and AISP services for a time of [X hours] before our provider was able to identify and apply a fix. We became aware of the issue at [X time] on [X date] when one of the AISPs notified us via our frontline support channel and this was escalated to our technical team at [Y time]. Working with our TPP community, our technical team identified the source of the issue at [Z time] and notified our provider. Their investigations revealed that a recent critical security patch had caused a network component to operate outside of expected parameters, and they began to work to resolve the

Ref	Question	Points to note and illustrative examples
		issue. Working over the weekend, they were able to re-patch their systems and restore functionality. Due to the criticality of the patch, and the risk that it posed to our customers if rolled-back (which could have resulted in all of our customer accounts becoming vulnerable to security risk), we were unable to resolve the issue within the previously published SLAs. We communicated this item to our onboarded TPPs via email. We also notified OBIE who then informed the wider ecosystem via their central noticeboard facility. These TPPs were able to notify their users of these services, assure them of our commitment to protecting them, and point them towards other methods of payment for them to use for any immediate needs.

Form B - Design of the dedicated interface

			Column A	Column B	
	Article	**Requirement**	**Description of the functional and technical specifications** **[Where relevant, also reference to the specific market initiative API specification used to meet this requirement and the results of conformance testing attesting compliance with the market initiative standard]**	**Summary of how the implementation of these specifications fulfils the requirements of PSD2, SCA-RTS and FCA Guidelines** **[Where relevant, any deviation from the specific market initiative API specification which has been designed to meet this requirement]**	**If not in place at the time of submission of the exemption request, when will the functionality be implemented to meet the requirement (must be before 14 September 2019).** **Has a plan for meeting the relevant requirements been submitted to the FCA alongside this form?**
1	PSD2 Article 67 SCA-RTS Article 30 RTS	Enabling AISPs to access the necessary data from payment accounts accessible online	We have implemented version 3.1 of the OBIE Account and Transaction API Specification which is designed to enable AISPs to obtain secure access to the necessary data within payment accounts that are accessible online. We have successfully run the OBIE Functional Conformance Tool for our implementation of the version 3.1 account access API and passed all required tests. The results of our conformance testing can be viewed here. [provide link and specify relevant part(s)]	As per PSD2 Article 67(1), our dedicated interface based on version 3.1 of the OBIE Standard enables the PSU to make use of account information services in relation to all the payment accounts we provide, which are accessible online. This includes: • [Bank X] Personal current account • [Bank X] Business current account • [Bank X] Personal credit card • [Bank X] Corporate credit card • [Bank X] Payment enabled savings account We provide detail on what information is available to AISPs via the dedicated interface in row 14. We consider that our dedicated interface, for access to the accounts above, meets relevant PSD2 requirements for ASPSPs pursuant to Article: 67(3)(a) which: *“…Enables secure*	

				communication with AISPs…”	
2	PSD2 Article 65, 66 & 67 SCA-RTS Article 30	Enabling provision or availability to the PISP, immediately after receipt of the payment order, of all the information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction	We have implemented version 3.1 of the OBIE Payment Initiation API Specification which enables provision and availability of information to the PISP immediately after receipt of the payment order from the PISP. According to the API specification the functionality of the POST operation enables the ASPSP to respond to submission of the payment order by providing information about the payment, including: • status • reference • amount of transaction in currency used • exchange rate • charges and breakdown of charges • date The status field enables the ASPSP to provide the PISP with different types of information relating to the payment order progress once it has been initiated by the PISP. For a single, immediate payment, we can respond with a status of ‘rejected’ or ‘pending’ or ‘accepted settlement in process’. Practically speaking, when the PISP initiates the payment order in order to satisfy the “immediate timeframe” of the regulatory requirement, in some instances, we may only be able to provide a status of ‘pending’. This means we have	Having implemented version 3.1, our dedicated interface enables the immediate provision and availability of ‘all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction’ as per PSD2 Article 66(4)(b). This covers the following accounts: • [Bank X] Personal current account • [Bank X] Business current account • [Bank X] Personal credit card • [Bank X] Corporate credit card • [Bank X] Payment enabled savings account The POST operation also enables the provision of information, immediately after receipt of the payment order, regarding the status of initiation of the payment order which will denote ‘pending’, “accepted settlement in progress” or “rejected” when the payment order is successfully received. The POST operation enables us to respond with the following information on the initiation of the payment order (where applicable) immediately after receipt of the payment order (in line with FCA Approach Document 17.29): • a reference enabling the payer to identify the payment transaction and, where appropriate, information relating to the payee • the amount of the payment transaction in the currency used in the payment	

			acknowledged receipt of the payment order which has been initiated via the PISP. This is a similar to the principle when the payer makes a payment directly – we confirm that the payment instruction has been received. Additionally, the API allows for TPPs to retrieve from us (via a GET) updates for each payment order, in the event the status changes after the payment order has been initiated. We have successfully run the OBIE Functional Conformance Tool on our implementation of the version 3.1 payment initiation API and passed all required tests. *The results of our conformance testing can be viewed here (provide link and specify relevant part(s))*	order • the amount of any charges for the payment transaction payable by the payer (to the payer's PSP) and, where applicable, a breakdown of the amounts of such charges • where an exchange rate is used in the payment transaction (by the payer's PSP) and the actual rate used in the payment transaction differs from the rate provided in accordance with regulation 43(2)(d) of the PSRs 2017, the actual rate used or a reference to it, and the amount of the payment transaction after that currency conversion • the date on which the PSP received the payment order The GET operation enables the provision of further information about the status of the payment order to be retrieved by the PISP. The PISP can periodically submit requests to us in order to obtain further status updates for example, if the PISP initially received a status of "pending" at payment initiation, this might be updated to either "accepted settlement in process" or "accepted settlement completed" or even "rejected".	

3	SCA-RTS Article 30(3)	Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations	The OBIE API Specifications we have implemented are based on RESTful JSON principles and all data models for request and response payloads map to ISO20022. The OBIE security model is based on the FAPI Profile of Open ID Connect, including but not limited to the following widely used international standards: • TLS 1.2 • OAuth2 • OpenID Connect (OIDC) • JWS • CIBA We have successfully run the OBIE functional conformance and security tools and passed all required tests. **The results of our conformance testing can be viewed here (provide link and specify relevant part(s))**	In line with SCA- RTS, Art. 30(3), these Standards follow widely used standards of communication used by both established financial institutions and third party developers, and issued by international and European standard bodies: • JSON (JavaScript Object Notation) is an open-standard file format that uses human-readable text to transmit data objects. It is a very common data format used for asynchronous communication including as a replacement for XML, and is defined by the Internet Engineering Task Force (IETF), see https://tools.ietf.org/html/rfc8259. • ISO20022 is the widely used standard for electronic data interchange between financial institutions. It describes a metadata repository containing descriptions of messages and business processes, see https://www.iso20022.org/. • The FAPI Security Profile is based on widely used security standards from the Open ID Foundation, see https://openid.net/foundation/	
4	PSD2 Article 64 (2) SCA-RTS Article 30(1) (c)	Allowing the payment service user to authorise and consent to a payment transaction via a PISP	The OBIE Standard, including the Customer Experience Guidelines (CEG) Chapter 4 describes how a PSU can consent and authorise a payment order via a PISP. The CEG defines two flows: • The PSU having consented with the PISP, the Redirect flow (CEG section 2.1) requires the PISP to redirect the PSU to the ASPSP to	Our implementation of the redirect flow complies with PSD2 Article 64(2) because it enables the PSU to give consent to the PISP and to authenticate via redirection, with the us [bank X]. As per SCA-RTS Article 30(1)(c) – as discussed above - the PISP is able to communicate securely to initiate a payment order from the payer's payment account and receive all information on the initiation of the payment	

			authenticate (via SCA unless an exemption applies). Once authenticated, the PSU is redirected back to the PISP and the PISP can subsequently initiate the payment order. [Optional if implemented] • The Decoupled flows (CEG section 2.3) allow the PSU to authenticate (via SCA on a separate device, unless an exemption applies). The PSU does not have to be redirected from the PISP interface/device. We have completed all required elements of the OBIE CEG Checklist regarding the Redirect Flow. The results of our conformance testing can be viewed here (provide link and specify relevant part(s))	transaction and all information regarding the execution of the payment transaction.	
5	PSD2 Article 66(3)(b) and 67(2)(b)	Enabling PISPs and AISPs to ensure that when they transmit the personalised security credentials issued by the ASPSP, they do so through safe and efficient channels.	We have implemented the OBIE Standard, which does not currently support Embedded flows (where credentials are given directly to the AISP or PISP). The Redirect and Decoupled flows in the OBIE Standard do not require the PSU's credentials to be shared with any third party provider.	N/A	
6	PSD2 Article 65(2)(c), 66(2)(d) and	Enabling the identification of the AISP/PISP/CBPII and support eIDAS for certificates	We accept eIDAS (both QWAC and QSEAL) certificates from TPPs as a means of identification for all communication sessions. These certificates could be issued by any	As per PSD2 and SCA-RTS Article 34 requirements, we accept eIDAS certificates from TPPs as a means of identification for all communication sessions. As per the EBA Opinion on the use of eIDAS	

	67(2)(c) SCA-RTS Article 30(1)(a) and 34		QTSP. We validate these certificates as follows: • We enable TPPs to identify themselves towards us by relying on these certificates for identification for each confirmation request, payment initiation and communication session. • For every TLS (secure communication) session, we check the validity of the TPP's eIDAS QWAC certificate using the relevant QTSP's OCSP service, via the Open Banking Directory. • We also check the regulatory status of each TPP on a regular basis using the Open Banking Directory.	certificates under the RTS, we accept both QWACs and QSEALCs.	
7	SCA-RTS Article 10(2) (b)	Allowing for 90 days re-authentication for AISPs	We have implemented the OBIE Account and Transaction API Specification v3.1 (section 5.3.3) which defines how customer re-authentication can take place for AISP redirection journeys. As part of this, we only issue AISPs with access tokens with a maximum life of 90 days. Once the 90 days have elapsed, the AISP no longer has access and must start a new authentication flow. This is also defined in the OBIE CEG v1.1 (section 3.1.2) which our	Our dedicated interface enables us to rely on the exemption in SCA-RTS Article 10(2), because the access tokens expire after 90 days has elapsed since the last time we applied SCA. We will apply SCA again to continue accessing information on the payment transactions executed in the last 90 days and/or balances.	

			implementation has followed.		
8	SCA-RTS Article 36(5)	Enabling the ASPSPs and AISPs to count the number of access requests during a given period	Our systems log and count the number of AISP requests for each PSU. However, we leave it up to AISPs to declare whether the PSU is present and to count the number of access requests for each PSU in a given 24 hour period and for the AISP to operate within the stated 4 times in a 24 period limit.	It is for AISPs to ensure compliance with SCA-RTS Article 36(5). We have not agreed a higher frequency of access requests with any AISPs as allowed by Article 36(5)(b).	
9	SCA-RTS Article 30 (4)	Allowing for a change control process	As per the OBIE OG, we notify PISPs, AISPs and CBPIIs (via the developer portal on our website) at least 3 months in advance of any changes to our API. We also provide backwards support for previous versions for at least 3 months. Therefore, any TPP will always have at least 3 months' notice before being required to update their systems as a result of any change to our dedicated interface.	Adopting these guidelines enables us to comply with SCA-RTS Article 30(4) which requires any change to the technical specification of their interface is made available to authorised PISPs, AISPs and CBPIIs, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance as soon as possible and not less than 3 months before the change is implemented (except for emergency situations).	
10	PSD2 Article 64(2) and 80(2) and 80(4)	Allowing for the possibility for an initiated transaction to be cancelled in accordance with PSD2, including recurring transactions	Version 3.1 of the OBIE API Specifications and CEG do not support the ability of the PSU to cancel PISP-initiated payment transactions by instructing the PISP. We do, however, allow cancellation of PISP-initiated payments, within the parameters of PSD2, within our PSU interface.	As per PSD2 Article 80(4), future dated PISP initiated payment transactions and recurring transactions can be cancelled as per PSD2 Article 78(2). PSUs have the ability to cancel these types of payments, within our direct channels, in the same way that they cancel these payments when set up directly by the PSU.	
11	SCA-RTS Article 36(2)	Allowing for error messages explaining the reason for the unexpected event or error	We have implemented version 3.1 of the OBIE API Specifications which utilises HTTP status codes to reflect the	The error codes provided by the OBIE API Specification, enable us, as per SCA-RTS Article 36(2), to send a notification message to	

			outcome of the API call (the HTTP operation on the resource). Furthermore, granular Functional Error Codes are specified (see section 5.1.3) as part of the API error response structure, and each of these has a more detailed explanation/reason. This specification includes a catalogue of error messages and rules around their use. The OBIE Read/Write API Specification v3.0 - Standard Error Codes are also available in section 7.3 of the CEG V1.1 In event of unexpected errors, we are able to send the following error messages to the TPP: • Identification: HTTP 401: Not Authorized or HTTP 503 Service Unavailable • Authentication: HTTP 401: Not Authorized • Exchange of data elements: Either the relevant HTTP 4xx error codes, and where possible a functional error code (e.g. Field Missing, Invalid Date, etc). We have successfully run the OBIE Functional Conformance Tool and passed all required tests, including examples for all error codes. The results of our conformance testing can be viewed here (provide link and specify relevant part(s))	the PISP or the AISP and the CBPII in the event of an unexpected event or error. The error codes explain the different reasons for the unexpected event or error, i.e.: • Not authorised • Service unavailable • Field missing • Invalid date	

12	PSD2 Article 19(6)	Supporting access via technology service providers on behalf of authorised actors	We have implemented the OBIE Standard recommendations for how a TPP could/should engage with Technical Service Providers (TSPs) i.e. businesses that obtains and processes payment account information in support of authorised or registered account information service providers but do not themselves provide the information to the user. • The OBIE Standard does not preclude any TPP using the services of a TSP, however, in all cases, the TSP should identify themselves to the ASPSP using the TPP's credentials (e.g. eIDAS certificate). • The Open Banking Directory (see https://www.openbanking.org.uk/providers/directory/) allows TPPs to include contact details for primary and secondary technical contacts (which could be the details of their TSP) and which can manage the TPP's credentials on behalf of the TPP. It also allows TPPs to create Software Statement Assertions (SSAs) which can be described as being managed by the TSP. • Furthermore, the Open Banking Directory allows a TPP to enter the details of an Agent on each SSA, using the 'on behalf of'	This supports TPPs in meeting their requirements under of PSD2 Article 19(6).	

			field. This field can then be used by TPPs and ASPSPs to display the name of the customer facing agent, in addition to the regulated party.		
13	PSD2 Article 97(5) and SCA-RTS Article 30(2)	Allowing AISPs and PISPs to rely on all authentication procedures issued by the ASPSP to its customers	We have implemented the OBIE Standard including the CEG which cover two different customer journeys, both allowing for PSU authentication with us – the Redirect Flow and the Decoupled Flow. Both these flows utilise the same credentials and user-interfaces that are available to PSUs when interacting directly with us in the direct channels. Further, on mobile devices the Redirect flow supports redirection from a TPP web page or TPP application to our application if already installed on the PSU device. This allows the PSU to use the same authentication experience as they would experience during a direct interaction with us. We have successfully completed all elements of the OBIE CEG Checklist. The results of our conformance testing can be viewed here (provide link and specify relevant part(s))	As per PSD2 Article 97(5) and SCA-RTS Article 30(2), our implementation of the OBIE Standard allows the AISP or PISP to rely on the authentication procedures provided us to the PSU. This approach is in line with FCA Approach Document, paragraph 17.134.	
14	PSD2 Article 67 (2) (d) and 30 (1) (b) and SCA-	Enabling the AISP to access the same information as accessible to the individual consumer and corporates in relation to their designated payment accounts and	Version 3.1 of the OBIE Account and Transaction API Specification is designed to enable ASPSPs to provide AISPs with account and transaction information.	As per SCA-RTS Article 36(1)(a), our implementation of version 3.1 of the OBIE Account and Transaction API enables us to provide AISPs with the same information from designated payment accounts and associated payment transactions made available to the	

	RTS Article 36 (1) (a)	associated payment transactions	Version 3.1 includes the following data fields: • Accounts (list of accounts associated with the PSU, including name of account holder) • Balances (list of balances for each account) • Transactions (list of transactions for a selected date range, including date, reference, amount) In addition, the specification provides AISPs access to: • Future Dated Payments • Direct Debits • Standing Orders • Beneficiaries • Statements (e.g. where transactions are grouped together within an overall statement) • Party (contact details for logged in user and/or name of account holder(s)) • Products (fees, charges and benefits relating to the account) We have successfully run the OBIE Functional Conformance Tool and passed all required tests. *The results of our conformance testing*	PSU when directly requesting access to the account information. AISPs can use the dedicated interface to access: information relating to the account, including: • the name(s) of the account holder(s) • the account number • transaction data, which is provided to the same level of granularity and covers the same time periods as is available to our customers when they access their account directly. This time period is [X years]. As per SCA-RTS Article 30(1)(b) the dedicated interface enables AISPs to communicate securely to request and receive information on our payment accounts. Secure communication is detailed further in row 19.	

			can be viewed here (provide link and specify relevant part(s)).		
15	SCA-RTS Article 36(1)(c)	Enabling the ASPSP to send, upon request, an immediate confirmation yes/no to the PSP (PISP and CBPII) on whether there are funds available	Version 3.1 of the OBIE Confirmation of Funds API Specification is designed to enable provision by the ASPSP of a "True" or "false" answer (which should be read as 'yes'/ 'no' answer) when a PISP or a CBPII submits to an ASPSP a request for confirmation of availability of funds on a PSUs payment account. We have successfully run the OBIE functional conformance tool and passed all required tests. *The results of our conformance testing can be viewed here (provide link and specify relevant part(s))*	Our implementation of version 3.1 of the OBIE Confirmation of Funds API Specification, enables us to comply with SCA-RTS Article 36(1)(c). As per paragraph 22 of the *EBA Opinion on the implementation of the RTS on SCA and CSC*, we have implemented this for requests from both CBPIIs and PISPs. For CBPIIs, once the PSU has provided us with their explicit consent for a particular CBPII (as per PSD2 Article 65(1)(b)), upon receipt of a confirmation of funds request from that CBPII, we respond immediately with a "true"="yes" or "false"= "no" answer for the amount in question. For PISPs, upon receipt of a confirmation of funds request, we respond immediately with a "true = yes" or "false" = "no" answer for the amount in question.	
16	PSD2 Article 97(2) and SCA-RTS Article 5	Enabling the dynamic linking to a specific amount and payee, including batch payments	We have implemented version 3.1 of the OBIE Payment Initiation API Specification, which is designed to provide PISPs with APIs to create (POST) a consent to make a payment and then subsequently (once the PSU has been authenticated) to initiate the payment. The standard results in the generation of a number of unique identifiers (e.g. payment id, the payment consent id, access token and a signature of the entire message body). These identifiers are bound to the payee and amount	As per PSD2 Article 97(2) our implementation of the OBIE Standard ensures that SCA for PIS includes elements which dynamically link the transaction to a specific amount and a specific payee. As per, SCA-RTS Article 5, we can confirm that: • the payer is made aware of the amount of the payment transaction and of the payee during the customer journey; • any change to the amount or the payee results in the invalidation of the authentication code generated.	

			when authentication takes place. Our implementation treats the message signature of the payment response message as the authorisation code used to dynamically link the payee and amount using a standard, cryptographic function. We have successfully run the OBIE Functional Conformance Tool and passed all required tests. The results of our conformance testing can be viewed here (provide link and specify relevant part(s))	Our implementation of the OBIE Standard is aligned with recital 4 of the SCA-RTS, i.e. dynamic linking is based on cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, and meeting the SCA-RTS security requirements.	
17	SCA-RTS Articles 30(2), 32(3), 18(2)(c)(v) and (vi) and 18(3)	Enabling the ASPSP to apply the same exemptions from SCA for transactions initiated by PISPs as when the PSU interacts directly with the ASPSP	For all payment types where we require a PSU to undergo SCA in our direct interface, we also require SCA via a PISP initiation. Where SCA is not required in the direct interface due to an exemption, SCA is not required for the equivalent payment via a PISP.	This approach is consistent with the SCA-RTS.	
18	SCA-RTS Article 4	Enabling strong customer authentication composed of two different elements	We have implemented redirection as part of our dedicated interface so that SCA is undertaken in our domain, rather than the TPPs domain. For all personal and business customers using mobile phones, we allow biometric authentication (as an ‘inherence’ factor) and device possession (as a ‘possession’ factor). In all other cases, including where a PSU does not have a mobile app, we require a combination of username and password (as ‘knowledge’ factor) and	As such, our dedicated interface enables SCA of PSUs that access their accounts via AISPs or initiate a payment via a PISPs or provide us with explicit consent to respond to specific CBPII confirmation of funds requests (prior to the first request). The SCA we require for PSUs accessing their via a TPP meets requirements of SCA-RTS Article 4, including compliance with PSD2 Article 97(1) – as the authentication is based on two or more elements which are categorised as knowledge, possession and inherence and SCA results in the generation of an authentication code (which meets SCA-RTS Article 4	

			one-time password via either SMS or Pin Sentry (as ‘possession’ factor). We apply this equally whether the PSU is accessing their account directly or via a TPP.	requirements).	
19	SCA-RTS Articles 28 & 35	Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII mitigating the risk for any misdirection of communication to other parties.	We have implemented the Open Banking Security Profile Implementer’s Draft v1.1.2 which is based on proven good practice of layered security. This profile requires the use of Mutually Authenticated TLS 1.2 at the transport layer to ensure that the two communicating parties can identify each other, specifically with the TPP using a QWAC eiDAS certificate. This communication channel is encrypted, to ensure that messages are only sent to the intended recipient and accordingly to minimise the risk of misdirection or interception. At the application layer, the profile utilises OpenID Connect to ensure that the two communicating parties are identified, and is based on the Open ID Foundation’s Financial Grade API (FAPI) security profile to further secure the layer. We also employ other mechanisms (such as message signing, using party identifiers in message headers) to provide a “defence in depth” against misdirected messages. We have successfully run the OBIE Security Conformance tool and passed	Our implementation of this specification ensures a secure data exchange between us and the PISP, AISP and CBPII and mitigates the risk for any misdirection of communication to other parties, as per SCA-RTS Articles 28 and 35.	

			all required tests. The results of our conformance testing can be viewed here (provide link and specify relevant part(s)).		
20	PSD2 Article 97(3) SCA-RTS Articles 30 (2)(c) and 35	Ensuring security at transport and application level	The OBIE Standard does not currently support Embedded flows. The Redirect and Decoupled flows in the standard do not require the PSU's credentials to be shared with any TPP.	As per PSD2, Article 97(3), we have robust measures in place to protect the confidentiality and integrity of payment service users' personalised security credentials. We have implemented redirection for authentication so the SCA-RTS Article 30(2)(c) obligation 'the integrity and confidentiality' of the personalised security credentials and of authentication codes transmitted by or through the PISP or the AISP shall be ensured' is not relevant.	
21	PSD2 Article 97(3) SCA-RTS Articles 22, 35 and 3	Supporting the needs to mitigate the risk for fraud, have reliable and auditable exchanges and enable providers to monitor payment transactions		As above, we have robust measures in place to protect the confidentiality and integrity of PSU's personalised security credentials. Other requirements are not relevant as the dedicated interface implements redirection. As per SCA-RTS Article 22, we mask security credentials when displayed to the PSU and do not store these in plain text. We also employ robust systems and processes to protect these and all secret cryptographic material. As per SCA-RTS Article 3, we perform a regular audit of our security measures and will make these available on request.	
22	SCA-RTS Article 29	Allowing for traceability	We have implemented Version 3.1 of the OBIE API Specification which requires that messages between PISPs and ASPSPs are digitally signed using	Our implementation of the standard enables us to meet SCA-RTS Article 29 requirements for traceability.	

			asymmetric key encryption. Under version 3.1, the PISP may use an eIDAS QSEAL or a private key that is lodged with the Open Banking Directory. This ensures that the signing key is available for verification and traceability for the foreseeable future. The signatures are generated for each request and response and provides cryptographic evidence that the messages were transmitted by the given PISP or ASPSP. Specifically, the signed response to each PISP request will inherently act as proof of receipt of the payment order, which will enable the PISP to log the date of this receipt. We have successfully run the OBIE Security Conformance tool and passed all required tests. The results of our conformance testing can be viewed here (provide link and specify relevant part(s))		
23	SCA-RTS Article 32	Allowing for the ASPSP's dedicated interface to provide at least the same availability and performance as the user interface	This is covered in Part A of this exemption form.	This is covered in Part A of this exemption form.	

While these illustrative answers have been drafted with regard to relevant regulatory provisions and best practice, they are not a complete list of the regulatory or legal obligations may apply. Although intended to be consistent with regulations and laws in the event of any conflict, applicable regulations and laws will take priority. Firms are responsible for their own compliance with all regulations and applicable laws when completing their individual applications. The contents of the illustrative answers do not constitute legal advice. The illustrative answers contained herein have been drafted in the context of the applicable OBIE Standard at the time of publication; Illustrative answers may need to be adapted and are subject to change, in accordance with the development and future releases of the Open Banking Standard, any changes or updates relevant to regulation, laws or regulator guidance, as well as, for practical considerations or improvements, where applicable.