CRYPTOASSETS (SAFEGUARDING) INSTRUMENT 2026

Powers exercised

A. The Financial Conduct Authority ("the FCA") makes this instrument in the exercise of the powers and related provisions in or under:

(1) the following powers and related sections in the Financial Services and Markets Act 2000 ("the Act"):

(a) section 137A (The FCA's general rules);
(b) section 137T (General supplementary powers);
(c) section 138D (Actions for damages); and
(d) section 139A (Power of the FCA to give guidance); and

(2) the other powers and related provisions listed in Schedule 4 (Powers exercised) to the General Provisions of the FCA's Handbook.

B. The rule-making provisions listed above are specified for the purposes of section 138G(2) (Rule-making instruments) of the Act.

Commencement

C. This instrument is one of a series of instruments which introduce or amend provisions of the Handbook relating to cryptoassets. These instruments all come into force on 25 October 2027, immediately after one another, in the following order:

(1) Glossary (Cryptoassets) Instrument 2026;
(2) Cryptoassets (Stablecoins) Instrument 2026;
(3) Cryptoassets (Admission of Qualifying Cryptoassets to Trading and Offers of Qualifying Cryptoassets to the Public) Instrument 2026;
(4) Cryptoassets (Market Abuse) Instrument 2026;
(5) Cryptoassets (Intermediaries) Instrument 2026;
(6) Cryptoassets (Trading Platforms, Transparency and Records) Instrument 2026;
(7) Cryptoassets (Lending, Borrowing and Staking) Instrument 2026;
(8) Cryptoassets (Safeguarding) Instrument 2026;
(9) Cryptoassets (Client Assets Consequentials) Instrument 2026;
(10) Cryptoassets (Conduct and Firm Standards) Instrument 2026; and
(11) Cryptoassets (COREPRU and CRYPTOPRU) Instrument 2026.

Amendments to the Handbook

D. The Client Assets sourcebook (CASS) is amended in accordance with the Annex to this instrument.

Notes

E. In the Annex to this instrument, the notes (indicated by "*Editor's note*:") are included for the convenience of readers but do not form part of the legislative text.

Citation

F. This instrument may be cited as the Cryptoassets (Safeguarding) Instrument 2026.

By order of the Board
25 June 2026

Annex

Amendments to the Client Assets sourcebook (CASS)

In this Annex, underlining indicates new text and striking through indicates deleted text, unless otherwise stated.

6 Custody rules

6.1 Application

6.1.1 R This chapter (the *custody rules*) applies to a *firm*:

…

(1B) when ~~it is *safeguarding and administering investments*~~, in the course of business that is not *MiFID business*~~;~~, it is:

(a) *safeguarding and administering investments*;

(b) *safeguarding cryptoassets* which are *relevant specified investment cryptoassets* and which do not belong to the *firm*; or

(c) *arranging cryptoasset safeguarding* in relation to *relevant specified investment cryptoassets*;

…

[*Editor's note*: CASS 6.1.1-AR is deleted and has been moved to CASS 6.1.1-DR.]

6.1.1-A R ~~In applying the *custody rules* to a *small AIFM's excluded custody activities*, any reference to a *firm* carrying on the *regulated activities* of *safeguarding and administering investments*, *safeguarding and administering assets (without arranging)* or *arranging safeguarding and administration of assets* includes those *excluded custody activities* that would, but for the exclusion in article 72AA of the *RAO*, amount to whichever of those *regulated activities* is referred to.~~ [deleted]

6.1.1-B R (1) In applying the *custody rules* to a *firm's* activities under *CASS* 6.1.1R(1B)(b) or *CASS* 6.1.1R(1F), any reference in the *custody rules* to *safeguarding and administering investments* or *safeguarding and administration of assets (without arranging)* should be read as including *safeguarding cryptoassets* which are *relevant specified investment cryptoassets*.

(2) In applying the *custody rules* to a *firm's* activities under *CASS* 6.1.1R(1B)(c), any reference the *custody rules* to *arranging safeguarding and administration of assets* should be read as

including *arranging cryptoasset safeguarding* in relation to *cryptoassets* which are *relevant specified investment cryptoassets*.

6.1.1-C G (1) The effect of *CASS* 6.1.1-BR is to extend the requirements in the *custody rules* to *safeguarding cryptoassets* and *arranging cryptoasset safeguarding*, in either case in so far as they relate to *relevant specified investment cryptoassets*.

(2) This has the effect that, for the purposes of applying the *custody rules* (but for no other purposes):

(a) the provision at Article 40(4) of the *RAO* inserted by Article 40(6) of SI 2026/102 should be disregarded; and

(b) even where the *firm* is not providing any 'administration' services for the *relevant specified investment cryptoassets* in respect of which it is *safeguarding cryptoassets*, the requirements of the *custody rules* would still apply to it in relation to that *safeguarding cryptoassets* activity.

(3) *CASS* 6.1.1-BR should be read as altering the meaning of any *Glossary* definition that is relevant to interpreting the *custody rules*, as well as altering the scope of the requirements in those *rules*.

(4) The reference to a *small AIFM's excluded custody activities* in *CASS* 6.1.1R(1F) is also affected by *CASS* 6.1.1-BR(1). This means that *CASS* 6 applies to a *small AIFM's* activity of *safeguarding cryptoassets* which are *relevant specified investment cryptoassets* despite the exclusion in article 72AA of the *RAO*.

6.1.1-D R In applying the *custody rules* to a *small AIFM's excluded custody activities*, any reference to a *firm* carrying on the *regulated activities* of *safeguarding and administering investments*, *safeguarding and administering assets (without arranging)* or *arranging safeguarding and administration of assets* includes those *excluded custody activities* that would, but for the exclusion in article 72AA of the *RAO*, amount to whichever of those *regulated activities* is referred to.

Insert the following new chapter, CASS 17, after CASS 16 (Stablecoin backing assets). All the text is new and is not underlined.

17 Cryptoasset safeguarding rules

17.1 Application

17.1.1 R Subject to *CASS* 17.1.3R, this chapter (the *cryptoasset safeguarding rules*) applies to a *firm* in relation to *regulated activities* carried on by it from an *establishment* in the *UK*.

17.1.2 G (1) Specific sections within the *cryptoasset safeguarding rules* have a narrower application than that set out in *CASS* 17.1.1R.

(2) *CASS* 17.3 (Cryptoasset safeguarding trusts) applies to a *firm* when it is *safeguarding cryptoassets*. The *rule* at *CASS* 17.3.3R requires the *firm* to act as a trustee when it is *safeguarding cryptoassets*, subject to certain exceptions which are set out in subsequent *rules* in that section. The *rule* at *CASS* 17.3.20R permits the *firm* to hold other *cryptoassets* within the same trust or trusts, as an *operational surplus*, and subject to certain conditions. *Cryptoassets* that are required or permitted to be in trust under those provisions of *CASS* 17.3 (Cryptoasset safeguarding trusts) are termed '*client cryptoassets*' in the *cryptoasset safeguarding rules*.

(3) *CASS* 17.2 (General safeguarding requirements), *CASS* 17.4 (Means of access) and *CASS* 17.5 (Records of cryptoassets and reconciliations) apply to a *firm* when it is, as a trustee under *CASS* 17.3.3R, *safeguarding cryptoassets* which are *client cryptoassets* (and therefore including any *operational surplus* that is permitted under *CASS* 17.3.20R).

(4) In addition, *CASS* 17.2 (General safeguarding requirements) and *CASS* 17.4 (Means of access) apply to a *firm* when it is *safeguarding cryptoassets* but not treating them as *client cryptoassets*, in reliance upon *CASS* 17.3.12R.

(5) *CASS* 17.6 (Appointing third parties to safeguard cryptoassets) applies to a *firm* when it is both *safeguarding cryptoassets* and *arranging cryptoasset safeguarding* in relation to the same *client cryptoassets*.

(6) *CASS* 17.7 (Arranging cryptoasset safeguarding) applies to a *firm* when it merely *arranges cryptoasset safeguarding*.

17.1.3 R This chapter does not apply to a *UK QCATP operator* which is an *overseas firm* and whose *Part 4A permission* for *cryptoasset safeguarding* is subject to a *requirement* (or a requirement imposed under section 55L(5) of the *Act*) to:

(1) not carry on the *regulated activity* of *cryptoasset safeguarding* other than by having control of *qualifying cryptoassets* to facilitate the settlement of transactions executed on a *UK QCATP*; and

(2) in the course of carrying on the *regulated activity* of *cryptoasset safeguarding* in accordance with (1), not accept any *qualifying cryptoassets* from any *UK* user other than *qualifying cryptoassets* received via a member of its *group* who is subject to, and acting in accordance with, *CASS* 17.3.5R.

17.1.4 G (1) The exemption at *CASS* 17.1.3R permits a *UK QCATP operator* whose settlement arrangements would involve the *regulated activity* of *cryptoasset safeguarding* (for example, because users of the *UK QCATP* have a right against the *UK QCATP operator* for the

return of *cryptoassets*) to not have to treat *qualifying cryptoassets* which it controls as part of those settlement arrangements as *client cryptoassets*.

(2) The exemption at *CASS* 17.1.3R only applies to a *UK QCATP operator* if its *Part 4A permission* is subject to a requirement, either at the *FCA's* own initiative or following the voluntary application by the *firm*, in the terms set out at *CASS* 17.1.3R(1) and (2).

(3) The effect of the part of that *requirement* which is set out at *CASS* 17.1.3R(2), together with *CASS* 17.3.5R, is to limit the amount of *qualifying cryptoassets* which would be owed to *UK* users in respect of which *CASS* 17 would not apply.

17.1.5 G (1) The defined term '*cryptoasset safeguarding class*' is an important concept in the *cryptoasset safeguarding rules* and *rules* related to *safeguarding cryptoassets* (for example, in the reporting requirements at *SUP* 16.35.7R). Examples and further *guidance* to show the effect of this term are set out below.

(2) For example, two *qualifying stablecoins* which are both instances of the same *qualifying stablecoin product* should not, for the purpose of the *cryptoasset safeguarding rules* and *rules* related to *safeguarding cryptoassets*, be considered to be in the same '*cryptoasset safeguarding class*' unless they exist on the same network that uses distributed ledger technology (eg, blockchain).

(3) Similarly, two *qualifying cryptoassets* should not be considered as falling within the same '*cryptoasset safeguarding class*' unless they are both instances of the same single product. This means that a *wrapped token* or a liquid staking token would not fall within the same '*cryptoasset safeguarding class*' as the relevant underlying *cryptoasset*.

(4) A consequence of this is likely to be that if a *firm* is carrying on *safeguarding cryptoassets* in relation to a *client cryptoasset* of a particular *cryptoasset safeguarding class*, it would not, without the *client's* agreement, be able to discharge its *safeguarding* obligations to its *client* by returning a *cryptoasset* that is identical to the one being *safeguarded* but for the fact that it exists on a different blockchain.

(5) Where the *cryptoasset safeguarding rules* require a *firm* to make a record or a notification that refers to a *cryptoasset safeguarding class*, the *firm* may be able to use the Digital Token Identifier system outlined in ISO standard 24165, provided that, in doing so, the relevant *cryptoasset safeguarding class* can be precisely distinguished.

Requirement to act compatibly with the Consumer Duty

17.1.6 R (1) When applying the *cryptoasset safeguarding rules* in relation to a *firm's retail market business*, the *firm* must act compatibly with the *Consumer Duty*.

(2) A contravention of (1) does not give rise to a right of action by a *private person* under section 138D of the *Act* (and *CASS* 17.1.6R(1) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

Exception for relevant specified investment cryptoassets

17.1.7 R This chapter (the *cryptoasset safeguarding rules*) does not apply to a *firm* in relation to any *safeguarding cryptoassets* activity or any *arranging cryptoasset safeguarding* activity where the *cryptoassets* in respect of which the *firm* is carrying on *safeguarding cryptoassets* or *arranging cryptoasset safeguarding* (as applicable) are *relevant specified investment cryptoassets*.

17.2 General safeguarding requirements

17.2.1 R This section applies to a *firm* when it is:

(1) *safeguarding cryptoassets* which are *client cryptoassets*; or

(2) *safeguarding cryptoassets* which would be *client cryptoassets* but are not being treated by the *firm* as *client cryptoassets* in reliance upon *CASS* 17.3.12R.

Requirement for adequate organisational arrangements

17.2.2 R A *firm* must, when *safeguarding cryptoassets*, introduce and maintain adequate organisational arrangements to:

(1) protect the relevant *client's* rights in relation to the *cryptoassets*, including in the event of the *firm's* insolvency; and

(2) minimise the risk of the loss or diminution of the *cryptoassets*, or of the rights in connection with those *cryptoassets*, as a result of the misuse of the *cryptoassets*, fraud, poor administration, inadequate record-keeping or negligence.

17.3 Cryptoasset safeguarding trusts

17.3.1 R This section applies to a *firm* when it is *safeguarding cryptoassets*.

Context and purpose

17.3.2 G (1) The scope of the *regulated activity* of *safeguarding cryptoassets* covers a range of legal relationships between the *firm* and the *client* in relation to a *qualifying cryptoasset* or *relevant specified investment cryptoasset*. It does not only apply where a *cryptoasset* that is controlled by a *firm* belongs to a *client*.

(2) Where the other conditions of the scope of the activity are met, the *regulated activity* of *safeguarding cryptoassets* is carried on in cases where the *person* on whose behalf the *firm* is safeguarding is the beneficial owner of the *cryptoasset*, and also in certain cases where that *person* has a right against the *firm* for return of a *cryptoasset*. The scope of the *regulated activity* for the latter type of case (where that *person* has a right for return) depends on whether the *firm* and that *person* have entered into a 'title transfer collateral arrangement' or repurchase agreement and on whether that *person* is a 'consumer' (as those terms are defined at Article 9N(5) of the *RAO*).

(3) The purpose of this section is to:

(a) set out a general requirement which would prohibit a *firm* from carrying on the *regulated activity* of *safeguarding cryptoassets* under any of those sorts of legal relationships that are within the scope of that *regulated activity* other than as a trustee;

(b) provide certain exemptions to that requirement to act as a trustee, subject to particular conditions being met; and

(c) set out other more specific requirements which a *firm* must meet when that requirement to act as a trustee applies.

(4)

(a) In the following *guidance*, the *FCA* sets out its policy rationale for the requirements and exemptions in this section concerning trusts.

(b) It is important that, in line with the requirements in *CASS* 17.2, *clients'* rights to *cryptoassets* which are being *safeguarded* are adequately protected through the use of trusts which can withstand competing claims to those *cryptoassets*, for example in case of the insolvency of the *firm* which is carrying on the *regulated activity* of *safeguarding cryptoassets*. In the *FCA's* view, this has market integrity advantages in the context of section 1D of the *Act*.

(c) Furthermore, in the *FCA's* view, taking account of potential difficulties that a *client* may have in evidencing and asserting ownership claims to *cryptoassets* (particularly where the *firm* has full control over those *cryptoassets*), a trust arrangement has consumer protection advantages over other legal arrangements that might exist between a *client* and *firm* in the context of *safeguarding cryptoassets* (such as an absolute title transfer or an agency arrangement), in the context of section 1C of the *Act*.

(d) This general requirement to *safeguard cryptoassets* as a trustee is set out at *CASS* 17.3.3R.

(i) That *rule* requires a *firm* to agree with its *client* that the *firm* will act as a trustee, so that this should clear to the *client*.

(ii) That *rule* does not create a statutory trust; the *FCA* is of the view that *firms* to which that requirement applies should have some flexibility around how they create private trusts, subject to certain conditions being met (see *CASS* 17.3.14R to *CASS* 17.3.18G).

(iii) Detailed and up-to-date records are also mandatory (see *CASS* 17.3.19R).

(e) However, certain other services which *clients* may engage a *firm* which is carrying on the *regulated activity* of *safeguarding cryptoassets* to provide in relation to *cryptoassets* would not be compatible with *cryptoassets* being *safeguarded* on trust. This is provided for at:

(i) *CASS* 17.3.4R in relation to *qualifying cryptoasset lending*;

(ii) *CASS* 17.3.5R in relation to the settlement of transactions executed on a *UK QCATP*; and

(iii) *CASS* 17.3.6 in relation to other services.

(f) In addition, a *firm* may be released from the requirement to act as a trustee where its dealings with the relevant *client* would require that. This is provided for at:

(i) *CASS* 17.3.8R in relation to a *client's* instructions to transfer a *cryptoasset* to another *person* (including the *firm*); and

(ii) *CASS* 17.3.10R in relation to a *client's* indebtedness to the *firm*.

(g) Furthermore, the *FCA* is of the view that it is disproportionate to require a *firm* to be a trustee where it is engaged to only provide a backup solution where its *client* contemporaneously retains full control of the *cryptoasset* in question. This is provided for at *CASS* 17.3.12R.

(h) *Firms* should note that each of the exemptions referred to above are subject to conditions set out within those *rules*.

(i) Finally, and again provided certain conditions are met including that this is necessary in order to service *clients*, a *firm* may co-mingle 'house' *cryptoassets* in the same trust as *client cryptoassets*. See *CASS* 17.3.20R on *operational surpluses*.

Requirement to safeguard as a trustee

17.3.3 R (1) Unless otherwise permitted in this section, a *firm* must ensure that wherever it carries on the *regulated activity* of *safeguarding cryptoassets*, it does so as a trustee of the relevant *cryptoasset* under trust arrangements which comply with *CASS* 17.3.14R.

(2) In so far as the requirement in (1) applies, a *firm* must ensure that its *client* on behalf of whom it is *safeguarding cryptoassets* has agreed to the *firm safeguarding cryptoassets* as a trustee (for example in any written agreement required under *COBS* 8.1 (Client agreements: non-MiFID designated investment business)).

(3) A *firm* must ensure that its *client's* agreement under (2) addresses how the trust is to be established (for example in relation to legal title transferring to the *firm* pursuant to a transfer of the *cryptoasset* to the *firm's* control).

Exemption from acting as a trustee for cryptoasset lending

17.3.4 R (1) A *firm* is not required to *safeguard cryptoassets* as a trustee under *CASS* 17.3.3R or, if it is already carrying on *safeguarding cryptoassets* in respect of a *client cryptoasset* as a trustee under *CASS* 17.3.3R, the *firm* may cease to treat a *cryptoasset* as a *client cryptoasset*, where the *client* on behalf of whom the *firm* is carrying on *safeguarding cryptoassets* has engaged the *firm* to provide a *qualifying cryptoasset lending* service in relation to a *cryptoasset*.

(2) The exemption in (1) only applies during the period for which the *qualifying cryptoasset lending* service is being provided in relation to that *cryptoasset*.

(3) Once that *qualifying cryptoasset lending* service in relation to a *cryptoasset* has ended for any reason, including by prior agreement or if the *client* has exercised any right to require that service to cease in relation to a *cryptoasset*, the exemption in (1) no longer applies.

(4) A *firm* may not use the exemption in (1) in relation to any *cryptoasset* which represents *qualifying cryptoasset borrowing collateral*, whether the obligations which the *cryptoasset* secures are owed to the *firm* itself or to another *authorised person* who has, under *CRYPTO* 9.6.8R(1)(b), arranged for the *firm* to carry on the *regulated activity* of *safeguarding cryptoassets*.

Exemption from acting as a trustee for qualifying cryptoasset trading platforms

17.3.5 R A *firm* may cease to treat a *qualifying cryptoasset* as a *client cryptoasset* (and therefore cease to carry on *safeguarding cryptoassets* as a trustee of the *cryptoasset*) where:

(1) the *client* on behalf of whom the *firm* is *safeguarding* the *qualifying cryptoasset* is also a user of a *UK QCATP* operated by the *firm* itself or another *person* in the *firm's group*;

(2) that *client* is trading, or has made it clear to the *firm* that they intend to trade, with *qualifying cryptoassets* of that *cryptoasset safeguarding class* using that *UK QCATP*;

(3) as part of the day-to-day operation of that *UK QCATP*, the *UK QCATP operator* needs to take control of *qualifying cryptoassets* to facilitate the settlement of transactions executed on that *UK QCATP*;

(4) the *firm* has obtained the *client's* prior informed consent, in accordance with *CASS* 17.3.11R, to the *qualifying cryptoasset* ceasing to be a *client cryptoasset* in order for transactions executed on the *UK QCATP* in that *cryptoasset safeguarding class* to settle; and

(5) at all times, the amount of *cryptoassets* of a particular *cryptoasset safeguarding class* which the *firm* is not treating as *client cryptoassets* under this *rule* for the *client* does not exceed 2% of the total amount of *cryptoassets* of that particular *cryptoasset safeguarding class* which remain in the *firm's* trusteeship for that *client* under *CASS* 17.3.3R.

Exemption from acting as a trustee where necessary for other services

17.3.6 R (1) A *firm* is not required to *safeguard cryptoassets* as a trustee under *CASS* 17.3.3R or, if it is already carrying on *safeguarding cryptoassets* in respect of a *client cryptoasset* as a trustee under *CASS* 17.3.3R, the *firm* may cease to treat that *cryptoasset* as a *client cryptoasset*, where:

(a) the *client* on behalf of whom the *firm* is carrying on *safeguarding cryptoassets* has engaged the *firm* to provide a service (other than services described in *CASS* 17.3.4R or *CASS* 17.3.5R);

(b) in order to provide that service to the *client*, the *firm* has concluded that it is necessary:

(i) for the *firm* to have ownership of the *cryptoasset*; and/or

(ii) for the *firm* to effect a transfer of ownership of the *cryptoasset* to another *person*; and

(c) the *firm* has obtained the *client's* prior informed consent, in accordance with *CASS* 17.3.11R, to that transfer of ownership in order for the service to be provided.

(2) Where a service for which the *firm* has relied on (1) ends, or where it is no longer necessary for the *firm* or another *person* to have ownership of *cryptoassets*, the exemption in (1) no longer applies.

(3) For each distinct service for which the *firm* intends to rely on (1), and prior to providing that service to any *client*, the *firm* must make a record of the reasons for concluding that it is necessary for the *firm* to have ownership of *cryptoassets*, or to effect a transfer of ownership of *cryptoassets* to another *person*, in order to provide that service (the '*client cryptoasset trust exemption record*').

(4) For the purposes of (3), a service must be considered 'distinct' if it has different technical features, a different purpose, or a different type of risk to the *client* to a service which has already been assessed by the *firm*.

(5) The *firm* must retain each *client cryptoasset trust exemption record* made under (3) for a period of 5 years after it has stopped providing the relevant service.

(6) A *firm* may not use the exemption in (1) in relation to any *cryptoasset* which represents *qualifying cryptoasset borrowing collateral*, whether the obligations which the *cryptoasset* secures are owed to the *firm* itself or to another *authorised person* who has, under *CRYPTO* 9.6.8R(1)(b), arranged for the *firm* to carry on the *regulated activity* of *safeguarding cryptoassets*.

17.3.7 G (1) The reference to 'distinct' service in *CASS* 17.3.6R(3) should be interpreted on a granular basis, meaning that a *firm* should investigate and conclude that a transfer of ownership is necessary in relation to the specific features of the service. For example, if a *firm* intends to rely on *CASS* 17.3.6R(1) in order to carry on the activity of *arranging qualifying cryptoasset staking*, it should make a record under *CASS* 17.3.6R(3) for each staking protocol in relation to which it will provide services.

(2) For the purposes of *CASS* 17.3.6R(1), the term 'service' should not be limited to services which only comprise *regulated activities*.

Exemption from acting as a trustee to act on client instructions to transfer

17.3.8 R A *firm* may cease to treat a *cryptoasset* as a *client cryptoasset* where:

(1) the relevant *client* has given the *firm* an express and specific instruction to effect a transfer of an amount or value of their *client cryptoassets* to another *person*, to the *firm* or to the *client* themselves; and

(2) the *firm* has given effect to that instruction.

17.3.9 G (1) The reference to an 'express and specific instruction' at *CASS* 17.3.8R(1) means that the *rule* cannot be relied on where the *client* has given the *firm* a mandate in relation to their *client cryptoassets* without any specific instruction for any particular transfer (for example, a discretionary investment mandate). For such a service where there is no express and specific *client* instruction, a *firm* may be able to rely on *CASS* 17.3.6R provided that the conditions in that *rule* are met.

(2) Following a transfer under *CASS* 17.3.8R to another *person* (the 'transferee'), the *firm* would be required to continue to *safeguard cryptoassets* in accordance with the requirements in this section if it is carrying on the *regulated activity* of *safeguarding cryptoassets* on behalf of the transferee in relation to that *cryptoasset*. This may mean that the *firm* will be required to *safeguard cryptoassets* as a trustee on behalf of the transferee.

Exemption from acting as a trustee where the client is indebted to the firm

17.3.10 R A *firm* may cease to treat a *cryptoasset* as a *client cryptoasset* where:

(1) the relevant *client* has given the *firm* a right, through a written binding agreement, to take ownership of their *cryptoassets* in order to discharge an obligation that the *client* owes to the *firm*; and

(2) the *firm* has exercised that right in accordance with the terms of that written agreement in relation to those *client cryptoassets*.

Obtaining a client's consent

17.3.11 R (1) This *rule* sets out steps which a *firm* must take in the course of obtaining a *client's* prior informed consent under *CASS* 17.3.5R(4) or *CASS* 17.3.6R(1)(c).

(2) For any *retail market business*, the *firm's* process for obtaining prior informed consent must be compatible with the *Consumer Duty*.

(3) In the course of seeking consent, the *firm* must specifically and clearly explain to the *client* the risks to the *client* of the *cryptoasset* not being within a trust, including in the event of the *firm's failure*.

(4) Any consent provided by a *client* must be obtained in writing and a record of it (the '*client cryptoasset trust exemption consent record*') must be retained for a period of 5 years after the *firm* has stopped relying on the consent to use the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1), as applicable.

(5) If a *client* withdraws their consent, the *firm* can no longer rely on the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1), as applicable, from the time at which the *client's* withdrawal of consent takes effect (taking into account any agreed notice period).

(6) A contravention of (2) does not give rise to a right of action by a private person under section 138D of the *Act* (and *CASS* 17.3.11R(2) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

(7) A contravention of any other aspect of this *rule* is not affected by (6).

Exemption from acting as a trustee where providing a backup solution

17.3.12 R A *firm* is not required to *safeguard cryptoassets* as a trustee under *CASS* 17.3.3R where all the following conditions are met:

(1) the *firm* has good reason to believe that the *client* on whose behalf the *firm* is carrying on *safeguarding cryptoassets* in respect of a particular *cryptoasset* has its own *means of access* which would enable the *client* to transact using the *cryptoasset* without relying on the *firm*;

(2) where that *client* is a *firm* that is itself also carrying on *safeguarding cryptoassets* in relation to that *cryptoasset*, that *client* has confirmed to the *firm* to which this *rule* applies that it is itself carrying on *safeguarding cryptoassets* in respect of that *cryptoasset* as a trustee under *CASS* 17.3.3R (as it applies to that *client*);

(3) the *firm* has not been appointed to provide any service in relation to that *cryptoasset* other than:

(a) undertaking one or more of the activities set out at *CASS* 17.4.2R in relation to the relevant *means of access* to the *cryptoasset* for which it is carrying on *safeguarding cryptoassets*; and

(b) undertaking those activities at *CASS* 17.4.2R only for the purposes of assisting the *client* in the event that the *client's* own *means of access* becomes lost, inoperable, inaccessible or irrecoverable; and

(4) when carrying on that limited *safeguarding cryptoassets* service, the *firm* does not also carry on the activity of *arranging cryptoasset safeguarding* in relation to that *cryptoasset*.

17.3.13 G (1) It may be possible for a *firm* to rely on the exemption at *CASS* 17.3.12R where it has been appointed to provide a backup and recovery solution for a *client* (and no other service).

(2) The *client* in the situation described in (1) may itself be another *firm* (or an unauthorised *cryptoasset* service provider) which has engaged the *firm* to provide that backup and recovery solution in order to make its own service more robust. The condition at *CASS* 17.3.12R(2) is only relevant where the *client* is a is another *firm* which is itself carrying on *safeguarding cryptoassets* in respect of the relevant *cryptoasset*.

(3) Where the *client* is another *firm* which is not carrying on *safeguarding cryptoassets* in respect of the relevant *cryptoasset* (for example, because it owns the *cryptoasset* outright for the purposes of *dealing in qualifying cryptoassets as principal*, and no other *person* has a right for the return of it) then the condition at *CASS* 17.3.12R(2) would not be relevant.

(4) Likewise, where the *client* is simply the investor in the *cryptoasset* (and provides no service to any other *person*) then the condition at *CASS* 17.3.12R(2) would not be relevant.

(5) To meet the condition at *CASS* 17.3.12R(1), it should not be necessary for the *firm* to prove (cryptographically or otherwise) that the *client* has their own *means of access*, but the *firm* should be able to explain the basis of its belief that the *client* is in that position. For example, this may be a point which is addressed in the *firm's* agreement with the *client*.

(6) The *client's* own *means of access* referred to at *CASS* 17.3.12R(1) may be a duplicate copy of the *firm's means of access* or may be an alternative *means of access* which co-exists with the *firm's means of access*.

Setting up and operating client cryptoasset trusts

17.3.14 R For any *client cryptoasset*, the *firm* must ensure that:

(1) the trust that is required under *CASS* 17.3.3R is created and operated by the *firm* in accordance with applicable legal requirements for trusts in the *UK*;

(2) the terms of any such trust are clearly documented with the effect that it is clear the trust is intended and it is clear what the terms are; and

(3) the terms and operation of the trust by the *firm* deliver the objectives and include the provisions set out in *CASS* 17.3.17R.

17.3.15 G To comply with *CASS* 17.3.14R(2) a *firm* may, for example, execute a deed or similar formal instrument.

17.3.16 R A *firm* must retain any document required under *CASS* 17.3.14R(2) setting out the terms of a trust, and details of any amendments which were made to the terms after the trust was first created, from the point at which the trust is created or the terms of the trust amended, and until 5 years after the trust has been brought to an end.

17.3.17 R A *firm* must ensure that the terms and operation of any trust that is required under *CASS* 17.3.3R deliver the objectives at (1) and (2) and include the provisions at (3) and (4):

(1) The *firm* must act as a trustee in relation to the *client cryptoassets* as well as in relation to any rights which can be exercised by virtue of the *firm safeguarding cryptoassets*, and in particular:

(a) the *firm* must be required to respond to the lawful instructions of the relevant *client* in relation to the *client cryptoassets*; and

(b) save for having the necessary powers to comply with any applicable *rules* or legal requirements, or unless otherwise agreed with the *client*, the *firm* must not have any discretion in applying, investing or otherwise using any *client cryptoassets* which are trust property.

(2) Subject to *CASS* 17.3.20R, the *firm's* operation of the trust ensures that the *client cryptoassets* within the trust are not co-mingled with, and are identifiable separately from, any other assets (for example, any assets for which the *firm* is not carrying on *safeguarding cryptoassets*, any assets for which the *firm* is relying on an exemption to act as a trustee under this section, and any assets which pertain to any other separate trust that is created to meet *CASS* 17.3.3R).

(3) Where there is, or is intended to be, more than one *client* on whose behalf the *firm* is *safeguarding cryptoassets* within a single trust, the terms of that trust must set out how any shortfalls in the trust, whether within a particular *cryptoasset safeguarding class* or across all *cryptoasset safeguarding classes* of *client cryptoassets* within the trust, are to be allocated between the *clients*.

(4) The terms of the trust must set out whether or not the *client cryptoassets* within the trust may be applied towards funding the distribution costs of the trust on the *failure* of the trustee and, if the terms do provide for this, the basis on which that funding will be deducted from the entitlements of the *clients*.

17.3.18 G (1) A *firm* should decide on an approach to settling and operating trusts under the *rules* in this section which is suitable for its business model, its *client* base and the types of *client cryptoassets* in respect of which it will be *safeguarding cryptoassets*. In particular:

(a) a *firm* may decide whether to operate separate trusts for each *client* or one or more 'omnibus' trusts for a particular class of *clients* (which may include all *clients*);

(b) a *firm* may decide whether to operate separate trusts for different *cryptoasset safeguarding classes*; and

(c) a *firm* may decide whether to operate separate trusts distinctly, using separate virtual addresses or devices, or to combine *client cryptoassets* at different virtual addresses or devices into the same trust.

(2) (a) A *firm* should consider whether the objective in *CASS* 17.3.17R(2) can be achieved through the use of different virtual addresses, with regard to the operation of the relevant network.

(b) A particular network relevant to a type of *client cryptoasset* may affect the choices available to a *firm* in deciding how to implement a trust which complies with the *rules* in this section.

(c) Where the network relies on another network for its functioning, a *firm* should ensure that the ownership of the *client cryptoassets* cannot be challenged or reversed through the operation of technology.

(d) Allocating *client cryptoassets* which exist at the same single virtual addresses or on the same single device into different trusts would not meet the requirement at *CASS* 17.3.17R(2) in relation to co-mingling.

(3) (a) A *firm* may decide how any shortfall in a trust should be allocated between *clients*, but in doing so, a *firm* should consider the requirement at *CASS* 17.1.6R.

(b) The *FCA* would generally expect a shortfall in a particular *cryptoasset safeguarding class* within a trust to be borne 'pro rata' by all *clients* for whom the *firm* is safeguarding *cryptoassets* of that particular *cryptoasset safeguarding class* in that particular trust, in proportion to their respective interests in those *cryptoassets*.

(4) The way in which a *firm* decides to set up its trust environment and the way in which it achieves the required segregation should be recorded in the *firm's client cryptoasset trust records*.

The client cryptoasset trust record

17.3.19 R (1) A *firm* must make and keep updated a record of each trust that it has created under *CASS* 17.3.3R which sets out the following details for that trust (the '*client cryptoasset trust record*'):

(a) a unique identifier code for the trust;

(b) the means by which the *firm* achieves the obligation at *CASS* 17.3.17R(2) including, where applicable:

(i) each relevant virtual address or device controlled by the *firm* at which *cryptoassets* pertaining to the trust are being safeguarded by the *firm*;

(ii) the name of each third party who has been appointed to *safeguard cryptoassets* pertaining to the trust under *CASS* 17.6; and

(iii) the identifier of the relevant network for the trust property;

(c) the name of each *client* who has an interest in the trust;

(d) the *cryptoasset safeguarding class(es)*in the trust, identified using the name of the *cryptoasset* or an identification code, in either case from which the relevant *cryptoasset safeguarding class* can be precisely distinguished;

(e) the location of the record of the terms of the trust required under *CASS* 17.3.16R;

(f) whether or not the *firm* has decided for the trust to include an *operational surplus* under *CASS* 17.3.20R; and

(g) if the trust has been brought to an end, the date of that occurring and the reason why it was brought to an end.

(2) A *client cryptoasset trust record* must be made at the same time as the relevant trust is created, and it must be updated immediately:

(a) upon making any changes to that trust; and

(b) as necessary following any *client cryptoasset reconciliation* under *CASS* 17.5.

(3) A *client cryptoasset trust record* must be retained for a period of 5 years after the relevant trust has been brought to an end.

Permitted operational surplus in trusts

17.3.20 R A *firm* may include, within any trust required to be created under *CASS* 17.3.3R, an amount of additional *qualifying cryptoassets* or *relevant specified investment cryptoassets* funded from the *firm's* own resources in order to meet the *firm's* operational needs (an '*operational surplus*'), provided the following conditions are met:

(1) An *operational surplus* in a trust is only permitted if it is necessary in order for the *firm* to provide services to one or more *clients* for whom the *firm* is *safeguarding cryptoassets*.

(2) Subject to (3), the *operational surplus* must be in the same *cryptoasset safeguarding class* as that in relation to which the *firm* is providing the services that necessitate the *operational surplus*.

(3) As an exception to (2), the *operational surplus* may be in a different *cryptoasset safeguarding class* where that would be necessary due to a technical limitation or feature of those services which the *firm* intends to provide.

(4) The amount of *cryptoassets* which form the *operational surplus* in any trust must not exceed a level that would be reasonably expected to be necessary, taking into account those services.

(5) The terms of the trust required under *CASS* 17.3.14R(2) and *CASS* 17.3.17R(3) must clearly set out that the *firm's* claim in the trust to the *operational surplus* in a particular *cryptoasset safeguarding class* is always and unconditionally subordinated to the claims of *clients* to *client cryptoassets* of that *cryptoasset safeguarding class* in the trust.

(6) When deciding to use a *operational surplus* in any trust that a *firm* operates under *CASS* 17.3.3R, the *firm* must make and retain a written record of the reason for the *operational surplus* to be necessary in order for the *firm* to provide services to one or more *clients* for whom the *firm* is *safeguarding cryptoassets* in the same trust (the '*per-trust operational surplus record*').

(7) The *firm* must not remove or reduce an *operational surplus* unless the amount removed represents an excess, and is removed following a *client cryptoasset reconciliation*, in accordance with *CASS* 17.5.12R.

17.3.21 R A *firm* must retain any *per-trust operational surplus record* made under *CASS* 17.3.20R(4) for a period of 5 years until after the *firm* ceases to use the *operational surplus* in that particular trust.

17.3.22 G (1) An example of where a *firm* may wish to use an operational surplus under *CASS* 17.3.20R(1) includes where the *firm's* service involves *qualifying cryptoasset staking* and, for example:

(a) it is necessary for the *firm* to contribute an amount of its own assets to meet the minimum threshold required by the staking protocol; or

(b) the staking rewards which are attributable to the *firm* (rather than any *client*) are received at a digital address pertaining to the trust.

(2) An example of where the exception at *CASS* 17.3.20R(3) may be relied on is to allow the *firm* to satisfy a requirement to pay transaction charges such as 'gas fees' in the *cryptoasset safeguarding class* that is required by the network when the transaction for which the *firm* is providing a service involves other *cryptoasset safeguarding classes*.

Guidance on trusts and appointing third parties

17.3.23 G (1) In cases where a *firm* appoints a third party to carry on the activity of *safeguarding cryptoassets* in accordance with *CASS* 17.6, the effect of *CASS* 17.3.3R and *CASS* 17.3.17R(1) means that the *firm's* contractual rights against that third party in relation to the relevant *client*

cryptoassets should be held on trust, because these are rights which can be exercised by virtue of the *firm safeguarding cryptoassets*.

(2) A *firm* in the position referred to in (1) should also comply with the other requirements of *CASS* 17.6.

17.4 Means of access

17.4.1 R This section applies to a *firm* when it is:

(1) *safeguarding cryptoassets* which are *client cryptoassets*; or

(2) *safeguarding cryptoassets* which would be *client cryptoassets* but are not being treated by the *firm* as *client cryptoassets* in reliance upon *CASS* 17.3.12R.

17.4.2 R The *rules* in this section apply where a *firm* undertakes any of the following activities in relation to the *means of access* to a *cryptoasset* in respect of which the *firm* is *safeguarding cryptoassets*:

(1) generating or creating the *means of access*, or any similar process;

(2) storing the *means of access*, in any form or medium of storage;

(3) exercising any form of control over the *means of access*;

(4) subjecting the *means of access* to any type of process; and

(5) destroying the *means of access*.

17.4.3 G (1) Because the *rules* in this section apply where a *firm* is *safeguarding cryptoassets*, this means that they do not apply where the *firm* does not have the requisite degree of 'control' as described at article 9N(4) of the *Regulated Activities Order*.

(2) The definition of *means of access* includes any means of which a *person* would need possession or knowledge to bring about a transfer of the benefit of a *cryptoasset* to another *person*.

(3) The scope of *CASS* 17.4.2R is broad and therefore the provisions in this section will apply to a range of activities and aspects of *safeguarding cryptoassets*, for example:

(a) using 'hot' or 'cold' devices or facilities to store the *means of access*;

(b) making and storing written records of the *means of access*; and

(c) processing the *means of access* by dividing a private cryptographic key into parts ('shards'), and (if relevant) distributing the shards amongst the *firm's* staff or other *persons* outside of the *firm*.

(4)

(a) If a *person* is, at a particular point in time, safeguarding only a single part of a private cryptographic key (eg, a 'shard') then, as a consequence of that fact by itself, they may be unlikely to have the requisite degree of 'control' as described at article 9N(4) of the *Regulated Activities Order* (assuming safeguarding just that one shard does not afford them the requisite degree of 'control' as described at article 9N(4)).

(b) However, if that *person* was previously in the position to create that shard and all the other shards from a private cryptographic key, then at that point they would have had the requisite degree of 'control' – even if after sharding the key they proceeded to distribute the other shards to other *persons*. Because they would have subjected the *means of access* to a process (the 'sharding' process), then as a result of *CASS* 17.4.2R(4) and the fact that they had the requisite degree of control at the time of the sharding, and assuming they are a *firm*, the requirements of this section would apply to that *firm*.

(c) Continuing from the example in (b) of a *firm* sharding a private cryptographic key and distributing it: if, after distributing the shards to other *persons* the *firm* can still require those other *persons* to return their shards under a binding agreement (or require their assistance to convene sufficient shards in order to digitally sign a transaction), then also as a result of *CASS* 17.4.2R(3), this section would apply to that *firm*.

(d) If any of the recipients of the shards had sufficient shards to themselves have the requisite degree of 'control' as described at article 9N(4) of the *Regulated Activities Order* then, assuming they are *firms*, as a result of *CASS* 17.4.2R(2), this section would apply to them also.

(5) In scenarios involving shards, the record required at *CASS* 17.4.8R(1)(d) should explain how the *firm* can exercise 'control', for example by setting out any relevant technical criteria which the *firm* is able to meet in order to digitally sign a transaction (such as a reconstruction or confirmation threshold), as well as how the *firm* is able to meet those criteria (for example, by a combination of retrieval from cold storage and requiring an appointed shard-holder to take certain steps).

17.4.4 R A *firm* must have robust security and organisational arrangements to ensure that, throughout the entire life cycle of any *means of access* to a *client cryptoasset*, the *means of access* are protected against the risks of inoperability, inaccessibility, loss, fraud and irrecoverability.

17.4.5 R A *firm* must promptly identify incidents of inoperability, inaccessibility, loss, fraud and irrecoverability to any *means of access* to a *client cryptoasset*.

17.4.6 R A *firm* must promptly resolve any incidents of inoperability, inaccessibility, loss, fraud and irrecoverability to any *means of access* to a *client cryptoasset*.

17.4.7 G In complying with *CASS* 17.4.4R to *CASS* 17.4.6R, a *firm* should, for example, consider whether, as relevant:

(1) its security and organisational arrangements adhere to any relevant international and industry standard practices;

(2) it is addressing any vulnerabilities to hacking and other risks of fraud and theft, including risks which originate from among the *firm's* own staff;

(3) it has a culture of detecting and acting on suspicious activity, including appropriate whistleblowing systems;

(4) it is addressing any:

(a) risks of 'single point of failure' (for example, as a result of a concentration of *means of access* with too few members of staff or on too few devices); and

(b) 'dependency risk' (for example as a result of distribution among too many members of staff or devices, or too much reliance on other *persons*);

(5) it has appropriate back-up and recovery systems;

(6) it has appropriate checks to ensure that the *means of access* remain accessible and operable, which themselves do not add undue security risks; and

(7) it employs random and non-deterministic methods as part of its security arrangements to minimise the risk of irreproducibility of any important data.

17.4.8 R (1) For each *means of access* that a *firm* controls at any particular point in time, and from the point at which the *firm* has such control, the *firm* must make and maintain a record which sets out the following information (the '*cryptoasset means of access record*'):

(a) the location (whether digital or physical) at which that *means of access* is being held including, where relevant, the virtual address for that *means of access*;

(b) a summary of the security measures which the *firm* has deployed for that *means of access* in accordance with *CASS*

17.4.4R, which must include the name of any other *persons* involved;

(c) the name of any natural *person*, such as a member of staff of the *firm*, who, to the *firm's* knowledge, is in a position to use that *means of access*;

(d) the way in which the *means of access*, whether by itself or in combination with other *means of access*, affords the *firm* 'control' over the relevant *cryptoasset* or *cryptoassets* in respect of which it is *safeguarding cryptoassets*; and

(e) whether the *means of access* has been destroyed (and, if so, when and the reason why it was destroyed).

(2) The *cryptoasset means of access record* under (1) must not contain or reproduce the *means of access* itself.

(3) The components of the *cryptoasset means of access record* under (1)(b) and (c) do not have to include the actual name of a *person* if doing so would compromise the *firm's* ability to comply with *CASS* 17.4.4R, provided that the record includes sufficient information from which the *person* can be identified using other records maintained by the *firm*.

17.4.9 R A *firm* must promptly update its *cryptoasset means of access records* required under *CASS* 17.4.8R as often as is necessary for the details within them to remain accurate.

17.4.10 R A *firm* must ensure that each *cryptoasset means of access record* is retained for a period of 5 years starting from whichever is the later of:

(1) the date it was created; or

(2) the date it was most recently modified.

17.4.11 R (1) A *firm* must create, retain and maintain a *means of access* policy document and a *means of access* procedures document which, taken together, explain the *firm's* means of complying with the requirements in *CASS* 17.4.4R to *CASS* 17.4.6R and *CASS* 17.4.8R to *CASS* 17.4.10R in clear and non-technical terms.

(2) A *firm* must review the documents under (1) at least once every year and make any necessary changes.

(3) A *firm* must retain each version of the documents required under (1) for a period of 5 years until after that version has been superseded by a new version.

17.5 Records of cryptoassets and reconciliations

17.5.1 R This section applies to a *firm* when it is *safeguarding cryptoassets* which are *client cryptoassets*.

General requirements

17.5.2 R A *firm* must keep such records as necessary to enable it at any time and without delay to distinguish *client cryptoassets* in respect of which the *firm* is *safeguarding cryptoassets* on behalf of one *client* from *client cryptoassets* in respect of which the *firm* is *safeguarding cryptoassets* on behalf of any other *client*, and from any *cryptoassets* which are not *client cryptoassets*.

17.5.3 R A *firm* must maintain its records in a way that ensures their accuracy, having regard to the business model of the *firm* and in particular the risks of:

(1) records becoming unreliable due to the nature of the *firm's* services and the networks relevant to the *client cryptoassets*; and

(2) the *firm* breaching the *rule* at *CASS* 17.3.3R.

17.5.4 R (1) A *firm* must establish and maintain systems and controls so that it can accurately determine the following and promptly identify and resolve any discrepancies in accordance with the *rules* in this section:

(a) for each trust that the *firm* has created under *CASS* 17.3.3R and in accordance with *CASS* 17.5.6R, the number of *client cryptoassets* of a particular *cryptoasset safeguarding class* in respect of which it is required to be *safeguarding cryptoassets* for a particular *client* (the *per-trust/client/class cryptoasset requirement*), taking into account its agreements with that *client* and any services that have been provided or are being provided to that *client*; and

(b) for each trust that the *firm* has created under *CASS* 17.3.3R and in accordance with *CASS* 17.5.7R, how many *client cryptoassets* of a particular *cryptoasset safeguarding class* it is *safeguarding cryptoassets* in relation to (the *per-trust/class cryptoasset resource*), whether itself or through the appointment of a third party under *CASS* 17.6.

(2) A *firm's* systems and controls under (1) must be designed to minimise the risks of inaccuracy, taking into account in particular:

(a) the time of day at which any processes to comply with *CASS* 17.5.6R to *CASS* 17.5.10R are run; and

(b) its arrangements for obtaining information from any third party appointed under *CASS* 17.6 in order to comply with *CASS* 17.5.7R.

(3) A *firm* must create, retain and maintain a reconciliations policy document and a reconciliations procedures document which, taken together, explain and set out:

(a) the *firm's* rationale for its procedures to comply with the *rules* in this section in clear and non-technical terms; and

(b) those procedures.

(4) A *firm* must review the documents under (3) at least once every year and make any necessary changes.

(5) A *firm* must retain each version of the documents required under (2) for a period of 5 years until after that version has been superseded by a new version.

17.5.5 G (1) Depending on the way a *firm* has complied with the *rules* in *CASS* 17.3, it may be necessary for the *firm*, when complying with the *rules* in this section, to make distinctions between different trusts that it has created under *CASS* 17.3.3R, and between different aspects of those trusts (such as whether or not it has decided for a particular trust to include an *operational surplus* under *CASS* 17.3.20R).

(2) When maintaining its records under the *rules* in this section, a *firm* should be making the distinctions referred to in (1) on the basis of its *client cryptoasset trust records*, which are required to be kept up to date under *CASS* 17.3.19R(2).

The per-trust/client/class cryptoasset requirement

17.5.6 R (1) A *firm* must calculate the *per-trust/client/class cryptoasset requirement* using the formula in (2) at least once each *business day*, with the result that, for each trust that the *firm* has created under *CASS* 17.3.3R, it produces, separately for each *client* that has an interest in that trust, the quantity of each *client cryptoasset* of each particular *cryptoasset safeguarding class* that the *firm* is required to hold for that *client* under that trust in accordance with the *rules* in *CASS* 17.3 (Cryptoasset safeguarding trusts).

(2) The *per-trust/client/class cryptoasset requirement* in (1) is calculated as (a) minus (b), where (a) and (b) are as follows:

(a) the sum of:

(i) the *firm's* previous *per-trust/client/class cryptoasset requirement* for the relevant trust, *client* and *cryptoasset safeguarding class*; and

(ii) the total of the following, each for the relevant trust:

(A) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *firm* has received from the *client* since the previous calculation;

(B) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *firm* has received on behalf of that *client* from any other *person* since the previous calculation;

(C) (to the extent not covered by (B)) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which have become due to the *client*, whether from the *firm* or earned in some other way, since the previous calculation; and

(D) (to the extent not covered by (B) or (C)) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which were required to be reinstated into the trust since the previous calculation under the *rules* at *CASS* 17.3 (Cryptoasset safeguarding trusts), including because of the end of a particular service; and

(b) the total of the following, each for the relevant trust:

(i) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *client* has withdrawn from the *firm* since the previous calculation;

(ii) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which the *firm* has transferred to another *person* on the *client's* instruction since the previous calculation;

(iii) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* which have become due to the *firm* since the previous calculation, in respect of which the *firm* has a right to take ownership of the *cryptoasset* under *CASS* 17.3.10R;

(iv) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* in respect of which the *firm* has relied on an exemption under *CASS* 17.3.4R, *CASS* 17.3.5R or *CASS* 17.3.6R to not hold the *cryptoassets* under the trust since the previous calculation;

(v) (to the extent not covered by (iii) or (iv)) the number of *client cryptoassets* of the relevant *cryptoasset*

safeguarding class which, since the previous calculation and as a result of services being provided by the *firm*, the *client* has been required to surrender; and

(vi) the number of *client cryptoassets* of the relevant *cryptoasset safeguarding class* in respect of which, following an unresolved shortfall, the *firm* has agreed with its *client* that it will no longer have to carry on *safeguarding cryptoassets*.

(3) A *firm* must use its internal records of *client* instructions, transactions and services to calculate any *per-trust/client/class cryptoasset requirement* under this *rule*, and must not use information from an external source (such as information contained on a blockchain or distributed ledger technology).

The per-trust/class cryptoasset resource

17.5.7 R (1) For each trust that a *firm* has created under *CASS* 17.3.3R, the *firm* must confirm the quantity of *client cryptoassets* of a particular *cryptoasset safeguarding class* in respect of which it is *safeguarding cryptoassets* under that trust at least once each *business day* (the '*per-trust/class cryptoasset resource*').

(2) The confirmation required under (1) must take account of both:

(a) the *client cryptoassets* of that particular *cryptoasset safeguarding class* which the *firm* can access in virtual addresses or devices; and

(b) where the *firm* has, under *CASS* 17.6, appointed a third party to carry on the activity of *safeguarding cryptoassets*, the *client cryptoassets* for which either:

(i) the third party has confirmed to the *firm* that it has the *means of access* to itself; or

(ii) in cases where that third party has appointed a further third party with the *firm's* consent under *CASS* 17.6.9R, the third party appointed by the *firm* has confirmed to the *firm* that the further third party has the *means of access* to.

(3) A *firm* must use external sources of information to confirm any *per-trust/class cryptoasset resource* under this *rule*, and must not use any internal source of information which the *firm* uses to calculate any *per-trust/client/class cryptoasset requirement* under *CASS* 17.5.6R

17.5.8 G (1) The requirements at *CASS* 17.5.6R(3) and at *CASS* 17.5.7R(3) are to ensure that a *firm's client cryptoasset reconciliations* use independent sources of information, with the effect that the *client cryptoasset*

reconciliations will be effective in their purpose of identifying discrepancies.

(2) A *firm* may use information from an external source such as information contained on the appropriate distributed ledger technology network to confirm the information described at *CASS* 17.5.7R(2)(a).

(3) Although information contained on a blockchain or distributed ledger technology may give an indication as to the information described at *CASS* 17.5.7R(2)(b), a *firm* should only use information provided from a third party appointed under *CASS* 17.6 in order to confirm that information.

(4) The requirements at *CASS* 17.5.6R(3) and at *CASS* 17.5.7R(3) should not prevent a *firm* from investigating and resolving any discrepancy under *CASS* 17.5.10R(3) or *CASS* 17.5.11R(1).

(5) When a *firm* is ascertaining the quantity for the *per-trust/class cryptoasset resource* under *CASS* 17.5.7R, it should not make any adjustment or allowance for *cryptoassets* in the relevant trust environment that may be part of an *operational surplus* which the *firm* has decided to include under *CASS* 17.3.20R.

17.5.9 R (1) Each time a *firm* calculates a *per-trust/client/class cryptoasset requirement* or confirms a *per-trust/class cryptoasset resource*, it must make a record of:

(a) the date and time it carried out that calculation or confirmation, as appropriate;

(b) the actions it took in order to carry out that calculation or confirmation, as appropriate; and

(c) the calculation result or confirmation outcome, as appropriate.

(2) A *firm* must retain each record made under (1) for a period of 5 years.

Client cryptoasset reconciliations

17.5.10 R (1) For each trust that a *firm* has created under *CASS* 17.3.3R, a *firm* must perform a *client cryptoasset reconciliation* under this *rule* at least once each *business day*, to check whether it has breached the *rules* in *CASS* 17.3 to hold *client cryptoassets* on trust.

(2) For each *cryptoasset safeguarding class* in respect of which the *firm* is required to be *safeguarding cryptoassets* within the relevant trust, the *firm* must compare the total of the *per-trust/client/class cryptoasset requirements* for all *clients* who have an interest in that trust with the *per-trust/class cryptoasset resource* for that trust at the same point in time.

(3) If the *firm* identifies a discrepancy as a result of carrying out a *client cryptoasset reconciliation*, it must promptly investigate the reason for the discrepancy and resolve it without delay or, where there is a shortfall, in accordance with *CASS* 17.5.13R.

(4) Each time a *firm* performs a *client cryptoasset reconciliation*, it must make a record (a '*client cryptoasset reconciliation record*') of:

(a) the date and time of the *client cryptoasset reconciliation*;

(b) whether or not the *client cryptoasset reconciliation* identified any discrepancies and, if so:

(i) the extent of them; and

(ii) the reasons for them; and

(c) any actions taken or attempted by the *firm* in relation to those discrepancies, including under *CASS* 17.5.12R and *CASS* 17.5.13R.

(5) A *firm* must retain each *client cryptoasset reconciliation record* made under (4) for a period of 5 years.

Other discrepancies

17.5.11 R (1) If a *firm* identifies a discrepancy related to its *safeguarding* of *client cryptoassets* outside of its processes for a *client cryptoasset reconciliation*, it must promptly investigate the reason for the discrepancy and resolve it without delay or, where there is a shortfall, in accordance with *CASS* 17.5.13R.

(2) Each time a *firm* identifies a discrepancy under (1), it must make a record (a '*client cryptoasset discrepancy record*') of:

(a) the date and time the discrepancy was identified;

(b) the reasons for the discrepancy and the extent of it; and

(c) any actions taken or attempted by the *firm* in relation to the discrepancy, including under *CASS* 17.5.12R and *CASS* 17.5.13R.

(3) A *firm* must retain each *client cryptoasset discrepancy record* made under (2) for a period of 5 years.

Client cryptoasset reconciliation excesses

17.5.12 R (1) This *rule* applies where a *firm's client cryptoasset reconciliation* for a particular trust shows that the *firm*, having investigated any discrepancies under *CASS* 17.5.10R(3) or *CASS* 17.5.11R(1), has confirmed there to be a greater amount of *cryptoassets* within that trust

for a particular *cryptoasset safeguarding class* than the total of the *per-trust/client/class cryptoasset requirements* for all *clients* who have an interest in that trust for that *cryptoasset safeguarding class*.

(2) Subject to (3), the *firm* must, before its next *client cryptoasset reconciliation* for that trust, remove all the excess *cryptoassets* of that particular *cryptoasset safeguarding class* from that trust.

(3) The *firm* may only retain excess *cryptoassets* of that particular *cryptoasset safeguarding class* within that trust if:

(a) it had previously decided to use an *operational surplus* in that trust and in that *cryptoasset safeguarding class* of *cryptoasset* in accordance with *CASS* 17.3.20R;

(b) the *firm's* retention of the excess does not cause the *firm* to be in breach of *CASS* 17.3.20R(2) or (3); and

(c) the amount of any excess that is withdrawn under this *rule*, and the amount of any excess that is retained under this *rule*, are recorded in the relevant *client cryptoasset reconciliation record* under *CASS* 17.5.10R(4)(c) or the relevant *client cryptoasset discrepancy record* under *CASS* 17.5.11R(2)(c), as appropriate.

Client cryptoasset reconciliation shortfalls

17.5.13 R (1) This *rule* applies where a *firm's client cryptoasset reconciliation* for a particular trust identifies a discrepancy as a result of, or that reveals, a shortfall which the *firm* has not yet resolved.

(2) A shortfall for the purposes of this *rule* is a situation for a particular trust under *CASS* 17.3.3R in which the *firm's per-trust/class cryptoasset resource* shows that there is a lesser amount of *cryptoassets* within that trust for a particular *cryptoasset safeguarding class* than the total of the *per-trust/client/class cryptoasset requirements* for all *clients* who have an interest in that trust in relation to that *cryptoasset safeguarding class*.

(3) This *rule* also applies where, outside of its processes for *client cryptoasset reconciliations*, a *firm* identifies a discrepancy as a result of, or that reveals, a shortfall which the *firm* has not yet resolved.

(4) The *firm* must address the shortfall by ensuring that, no later than 24 hours after identifying the discrepancy, the *firm* has the correct number of *client cryptoassets* on trust.

(5) Where necessary to comply with the requirement at (4), the *firm* must:

(a) appropriate its own *cryptoassets* in the relevant *cryptoasset safeguarding class*;

(b) acquire *cryptoassets* in the relevant *cryptoasset safeguarding class* using its own resources; or

(c) procure a third party appointed under *CASS* 17.6 to apply or acquire its own *cryptoassets* in the relevant *cryptoasset safeguarding class* to resolve the shortfall.

(6) Each measure taken by a *firm* to comply with (4) must be recorded in the relevant *client cryptoasset reconciliation record* under *CASS* 17.5.10R(4)(c) or the *relevant client cryptoasset discrepancy record* under *CASS* 17.5.11R(2)(c), as appropriate.

(7) A shortfall will not be considered to be addressed under (4) if *cryptoassets* of another *cryptoasset safeguarding class*, or some other type of asset (e.g. *money*), are placed in the trust.

17.5.14 G (1) *CASS* 17.5.13R does not prevent a *firm* from setting aside an alternative asset for the relevant *client(s)*, or paying/transferring an alternative asset to them, in an amount which would match any claim that they might have against the *firm* for the shortfall – for example, where doing so is required under the *firm's* agreement with the *client(s)*, is required by the *FCA*, or is considered by the *firm* to be required for another reason.

(2) Where a *firm* takes the action described in (1) involving an alternative asset, this does not have the automatic consequence that the *firm* will have addressed the shortfall as required under *CASS* 17.5.13R(4).

(3) However, it may put the *firm* and *client* in a position to agree that the *firm* need no longer carry on the activity of *safeguarding cryptoassets* in relation to the *cryptoassets* in shortfall, which may then be reflected in the *per-trust/client/class cryptoasset requirement* (see *CASS* 17.5.6R(2)(b)(vi)).

(4) In making any such agreement with a *client* in the course of *retail market business*, whether in advance or at the time of the shortfall, a *firm* should act compatibly with its obligations under the *Consumer Duty*.

17.5.15 R Where a *firm* fails to address a shortfall as required by *CASS* 17.5.13R, it must immediately:

(1) notify each affected *client* in writing (including those who are affected because they have an interest in the relevant trust which has, under the terms of that trust, reduced); and

(2) notify the *FCA* in writing, setting out:

(a) the reasons for the shortfall and the reasons for the *firm* failing to address it;

(b) the name of each *cryptoasset safeguarding class* of *cryptoasset* for which there is a shortfall, identified using the name of the *cryptoasset* or an identification code, in either case from which the relevant *cryptoasset safeguarding class* can be precisely distinguished, and the amount of that shortfall in that *cryptoasset safeguarding class*;

(c) the number of *clients* in the relevant trust affected by the shortfall and by how much each affected *client* is affected;

(d) the *firm's* expected timeframe for resolution of the shortfall, including detail on the steps which the *firm* and any third parties intend to follow to achieve resolution; and

(e) the approach the *firm* is taking in relation to *client* notifications under (1).

Other notification requirements

17.5.16 R A *firm* must notify the *FCA* in writing without delay if either of the following apply:

(1) its internal records relating to *safeguarding cryptoassets* are materially out of date, or materially inaccurate or invalid; or

(2) it will be unable, or materially fails, to comply with *CASS* 17.5.6R, *CASS* 17.5.7R or *CASS* 17.5.10R.

17.6 Appointing third parties to safeguard cryptoassets

17.6.1 R This section applies to a *firm* when it *safeguards cryptoassets* which are *client cryptoassets* and, in the course of carrying on that activity, it *arranges cryptoasset safeguarding*.

Purpose of this section

17.6.2 G (1) Where a *firm* carries on the activity of *safeguarding cryptoassets*, it may be necessary for the *firm* to appoint a third party to carry on the activity of *safeguarding cryptoassets* under the *firm's* direction in relation to a particular *client cryptoasset* or *client cryptoassets* of one or more *cryptoasset safeguarding classses*.

(2) That third party appointed by the *firm* may itself be a *firm* or may, for example, be a *person* who is *overseas* and who is not required to be *authorised* to carry on the activity of *safeguarding cryptoassets* in these circumstances.

(3) This section sets out the *rules* that apply to such an appointment by a *firm* of a third party to carry on that activity in order to address the risk of harm to the *firm's clients* that might result from that appointment, particularly in cases where the third party is not itself *authorised*.

(4) In the *FCA's* view, where a *firm* appoints a third party to carry on the activity of *safeguarding cryptoassets* in relation to any *client cryptoasset*, the *firm* will be carrying on the activities of both *safeguarding cryptoassets* and *arranging cryptoasset safeguarding*. In that situation, the *firm*, while remaining a trustee who is *safeguarding cryptoassets*, arranges for another *person* to *safeguard cryptoassets* under the *firm's* direction.

(5) The scenario described in (4) is different to one in which a *firm* only carries on *arranging cryptoasset safeguarding* and does not itself carry on *safeguarding cryptoassets*. In that situation, in making the arrangements which will result in the *client* receiving the service of *safeguarding cryptoassets* from another *person*, the *firm* is not itself a trustee of the *cryptoassets*.

(6) This section would not apply to the scenario described in (5) in which a *firm* only carries on *arranging cryptoasset safeguarding*. The *rules* in *CASS* 17.7 apply to a *firm* that only carries on *arranging cryptoasset safeguarding*.

(7) This section would not apply where the *firm* appoints a third party to hold part of a *means of access* where the third party would not be *safeguarding cryptoassets* because it lacks the requisite degree of 'control'. An example of this is where the *firm* appoints a third party to hold a shard of a private cryptographic key, but possession or knowledge of that shard, by itself, would not put the third party in a position to be able to transfer the benefit of the relevant *client cryptoasset*.

The conditions for appointing third parties to safeguard cryptoassets

17.6.3 R (1) A *firm* may appoint and retain another *person* (a 'third party') to carry on the activity of *safeguarding cryptoassets* in respect of which the *firm* has undertaken to its *client* to carry on *safeguarding cryptoassets*, but only if the following conditions are met:

(a) the third party operates in a jurisdiction which specifically regulates the safeguarding of *cryptoassets* through mandatory requirements concerning financial and operational resilience, security of the *means of access* to *cryptoassets*, and record-keeping, and the activities of the third party pursuant to the appointment by the *firm* are supervised in that jurisdiction;

(b) the *firm* has concluded, having completed the due diligence and any periodic review required under *CASS* 17.6.5R, that the appointment of the third party would not increase the risk of loss or diminution of any *client cryptoassets* which are subject to the arrangement, having regard to the *firm's* compliance with *CASS* 17.2.2R;

(c) in relation to a *firm's retail market business*, the appointment of the third party is compatible with the *Consumer Duty*;

(d) prior to the appointment commencing, the *firm* has entered into an agreement with the third party in the form required at *CASS* 17.6.6R; and

(e) the *firm* has met the governance requirements at *CASS* 17.6.9R.

(2) A contravention of (1)(c) does not give rise to a right of action by a private person under section 138D of the *Act* (and *CASS* 17.6.3R(1)(c) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

(3) A contravention of any other aspect of this *rule* is not affected by (2).

17.6.4 G (1) Where a *client* has instructed a *firm* to appoint a particular third party, the *firm* should still ensure that the conditions for the appointment at *CASS* 17.6.3R are met.

(2) To meet the condition at *CASS* 17.6.3R(1)(a) it is not essential that the mandatory requirements of the other jurisdiction refer to the specific terms mentioned in that requirement (e.g. 'financial and operational resilience', 'security of the *means of access* to *cryptoassets*', and 'record-keeping') provided that they focus on all of those aspects in substance.

Mandatory due diligence

17.6.5 R (1) A *firm* must exercise all due skill, care and diligence in the selection, appointment and periodic review of the third party and of the arrangements for the *safeguarding* of the relevant *client cryptoassets*, in order to conclude that the appointment of the third party would not increase the risk of loss or diminution of any *client cryptoassets* which are subject to the arrangement.

(2) When a *firm* makes the selection and appointment and conducts the periodic review referred to under this *rule*, it must take into account:

(a) whether the third party has the appropriate regulatory permissions to carry out the appointment;

(b) the arrangements that the third party has in place for *safeguarding cryptoassets*;

(c) the capacity and capability of the third party to provide the contracted services;

(d) the capital or financial resources of the third party;

(e) the creditworthiness of the third party;

(f) the potential impact on the contracted services of any other activities undertaken by the third party and, if relevant, any *affiliated company*;

(g) the expertise and market reputation of the third party;

(h) any legal requirements relating to the carrying on of *safeguarding cryptoassets* in respect of the relevant *cryptoassets* that could adversely affect the *firm's clients'* rights;

(i) market practices relating to the carrying on of *safeguarding cryptoassets* in respect of the *cryptoassets* that could adversely affect the *firm's clients'* rights;

(j) any relevant industry standard reports, including in relation to security; and

(k) where the third party appointed by the *firm* has appointed a further third party with the *firm's* consent under *CASS* 17.6.9R, all the factors set out above in relation to that further third party.

(3) The *firm* must conduct the periodic review required under this *rule* at least once each year.

The agreement condition

17.6.6 R A *firm* must have entered into a written agreement with any third party that it appoints to carry on the activity of *safeguarding cryptoassets* under *CASS* 17.6.3R. This agreement must, at minimum:

(1) set out the binding terms of the arrangement between the *firm* and the third party;

(2) be in force for the duration of the appointment;

(3) clearly set out the service(s) that the third party is contracted to provide;

(4) require the third party to seek and obtain the *firm's* written consent prior to the third party being able to appoint a further, different third party to carry on the activity of *safeguarding cryptoassets*;

(5) in recognition that the *firm* is acting as a trustee in relation to the *client cryptoassets* that are subject to the appointment:

(a) require that any *client cryptoassets* that are subject to the appointment are not co-mingled with, and are identifiable separately from, any assets belonging to the third party;

(b) require that any *client cryptoassets* that are subject to the appointment are not co-mingled with, and are identifiable separately from, any assets belonging to the *firm* for which it is not acting as a trustee;

(c) require that any *client cryptoassets* that are subject to the appointment are not co-mingled with, and are identifiable separately from, any assets pertaining to any other appointment;

(d) require the third party to recognise that the *firm* acts for its *clients* as trustee over the *client cryptoassets*; and

(e) exclude any rights of the third party to exercise set-off or counterclaim against the *client cryptoassets* in respect of any debt owed to it or to any other *person*;

(6) require the third party to notify the *firm* whenever *cryptoassets* are no longer subject to the terms of the agreement for any reason;

(7) include provisions detailing the extent of the third party's liability in the event of the loss of a *client cryptoasset* caused by the fraud, wilful default or negligence of the third party or an agent appointed by the third party; and

(8) set out the procedures and authorities for the passing of instructions to, or by, the *firm*.

17.6.7 R A *firm* must take the necessary steps to ensure that both it and the third party adhere to the agreement referred to at *CASS* 17.6.6R at all times.

Consenting to safeguarding chains

17.6.8 R (1) This *rule* applies where, under the mandatory term described at *CASS* 17.6.6R(4), a third party appointed by the *firm* seeks the *firm's* consent to itself appoint a further, different third party to carry on the activity of *safeguarding cryptoassets* in relation to *client cryptoassets* which the *firm* has undertaken to its *client* to *safeguard*.

(2) The *firm* must withhold the consent referred to in (1) unless it is satisfied that:

(a) the further appointee operates in a jurisdiction which specifically regulates the safeguarding of *cryptoassets* through mandatory requirements concerning financial and operational resilience, security of the *means of access* to *cryptoassets*, and record-keeping, and the activities of the further appointee are supervised in that jurisdiction;

(b) the *firm* has concluded, having completed due diligence on the further appointee in line with the requirements under *CASS* 17.6.5R, that the further appointment would not increase the

risk of loss or diminution of any *client cryptoassets* which are subject to the arrangement, having regard to the *firm's* compliance with *CASS* 17.2.2R;

(c) in relation to a *firm's retail market business*, the further appointment is compatible with the *Consumer Duty*; and

(d) the agreement under which the further appointment will be governed (as between the third party appointed directly by the *firm* and the further third party) contains terms which provide equivalent safeguards to those set out at *CASS* 17.6.6R(1) to (8).

(3) (a) The *firm* may approach its assessment under (2)(b) by requiring the third party it has appointed under *CASS* 17.6.3R to apply the factors set out at *CASS* 17.6.5R(2) in relation to the further appointee and to report its conclusions to the *firm*.

(b) Where a *firm* takes the approach in (a), it remains fully responsible for complying with the *rules* in this section in relation to the further appointment.

(4) Any consent given by the *firm* under this *rule* must be periodically reviewed, at least once each year.

(5) A contravention of (2)(c) does not give rise to a right of action by a private person under section 138D of the *Act* (and *CASS* 17.6.8R(2)(c) is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

(6) A contravention of any other aspect of this *rule* is not affected by (5).

The governance condition

17.6.9 R (1) Each proposed appointment by the *firm* of a third party under *CASS* 17.6.3R and each proposed consent under *CASS* 17.6.8R, together with the *firm's* considerations and conclusions to support that proposal, must be approved by the *firm's governing body* before the appointment is made or the consent is given, or by a *person* or *persons* within the *firm* to whom the *firm's governing body* has delegated that role (the '*governing body's* delegate').

(2) Where the *governing body* has delegated one or more *persons* for the purposes of the approval under (1), that delegation must include the *SMF manager* to whom the *firm* has appointed the *FCA-prescribed senior management responsibility* (Reference letter (z)) in the table in *SYSC* 24.2.6R (functions in relation to *CASS*).

(3) The outcome of each periodic review of a *firm's* selection and appointment of a third party that it conducts under *CASS* 17.6.5R, together with the *firm's* considerations and conclusions, must be

approved by the *firm's governing body* or the *governing body's* delegate within 3 *months* of the review being concluded.

Policy on appointing third parties

17.6.10 R (1) A *firm* must produce and maintain a written policy that sets out its methodology for any selections, appointments, periodic reviews and consents that are required under *CASS* 17.6.3R, *CASS* 17.6.5R and *CASS* 17.6.8R.

(2) A *firm* must retain the written policy under (1) until 5 years after it has been superseded by any new version of the written policy, or otherwise indefinitely.

Records

17.6.11 R (1) A *firm* must make a record of how the requirements of *CASS* 17.6.3R(1) or *CASS* 17.6.8R(2) are met in relation to any appointment of a third party under *CASS* 17.6.3R or consent to a further appointment of a third party under *CASS* 17.6.8R. That record must include the conclusions of any due diligence exercise carried out in accordance with those *rules*, making explicit reference to the factors set out at *CASS* 17.6.5R(2)(a) to *CASS* 17.6.5R(2)(j) (a '*client cryptoasset third party due diligence record*').

(2) A *firm* must make the record under (1) prior to the relevant appointment commencing or the relevant consent being given.

(3) Whenever a *firm* undertakes a periodic review of its selection and appointment of a third party under *CASS* 17.6.5R or of the *firm's* consent to an appointment under *CASS* 17.6.8R(4), the *firm* must make a record of the conclusions of its review, making explicit reference to the factors set out at *CASS* 17.6.5R(2)(a) to *CASS* 17.6.5R(2)(j) (a '*client cryptoasset third party review record*').

(4) A *firm* must make the record under (3) on the date it completes the review.

(5) A *firm* must make a record of each approval given by its *governing body* or its *governing body's* delegate under *CASS* 17.6.9R(1) or (3) (a '*client cryptoasset third party governance record*').

(6) A *firm* must make the record under (5) on the date of the *governing body's* or its *governing body's* delegate's approval.

(7) A *firm* must retain the records under (1), (3) and (5) until 5 years after the relevant appointment ceases.

17.7 Arranging cryptoasset safeguarding

17.7.1 R This section applies to a *firm* when it *arranges cryptoasset safeguarding*, but is not *safeguarding cryptoassets* in relation to which it is *arranging cryptoasset safeguarding*.

Agreements

17.7.2 R Each time a *firm*, on behalf of a *client*, *arranges cryptoasset safeguarding* with another *person*, it must enter into an agreement with that other *person*. This agreement must, at minimum:

(1) set out the obligations between the *firm* and the other *person*, including any ongoing obligations of the *firm*;

(2) set out the basis for any payments or other consideration between the two parties; and

(3) include provisions detailing the extent of either party's liability in the event of the loss of a *cryptoasset*.

Records

17.7.3 R (1) When a *firm arranges cryptoasset safeguarding*, it must ensure that proper records of the arrangements are made at the time the arrangements are put in place, and at the time the arrangements are amended (a '*cryptoasset safeguarding arrangement record*').

(2) A *firm* must retain the records made under (1) for a period of 5 years after they are made.

Amend the following as shown.

Sch 1 Record keeping requirements

…

Sch 1.3 G

Handbook reference	Subject of record	Contents of record	When record must be made	Retention period
…				
CASS 16.7.10R	…	…	…	…
CASS 17.3.6R(3)	*Client cryptoasset trust exemption record*	A record of a *firm's* reasons for concluding that it is necessary for the exemption at	Prior to providing the relevant service to any *client*	5 years after it has stopped providing the relevant service

		CASS 17.3.6R(1) to be used to provide a service		
CASS 17.3.11R(4)	*Client cryptoasset trust exemption consent record*	A record of a *firm's client's* written consent under *CASS* 17.3.5R(4) or *CASS* 17.3.6R(1)(c) for the *firm* to use the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1) respectively	Prior to making use of the exemption in relation to the *client's client cryptoasset*	5 years after it has stopped relying on the consent to use the exemption at *CASS* 17.3.5R(1) or *CASS* 17.3.6R(1)
CASS 17.3.16R	The document required under *CASS* 17.3.14R(2) setting out the terms of a trust (e.g. a deed)	The terms of the trust and details of any amendments which were made to the terms after the trust was first created	At the time the trust is created	5 years after the trust has been brought to an end
CASS 17.3.19R	*Client cryptoasset trust record*	Details of a trust that a *firm* has created under *CASS* 17.3.3R	At the time the *firm* creates the trust to which the *client cryptoasset trust record* pertains	5 years after the relevant trust has been brought to an end
CASS 17.3.21R	*Per-trust operational surplus record*	The reason for it being necessary for the *firm* to use an *operational surplus* for a particular trust created under *CASS* 17.3.3R	When the *firm* decides to use an *operational surplus* in a trust that the *firm* operates under *CASS* 17.3.3R	5 years until after the *firm* ceases to use the *operational surplus* in that particular trust
CASS 17.4.8R	*Cryptoasset means of access record*	Details of each *means of access* that the *firm* controls	When the *firm* starts to control the *means of access*	5 years after the later of the date the record was created and the date it was most

				recently modified
CASS 17.4.11R	Each version of a *firm's means of access* policy document and *means of access* procedures document	An explanation of the *firm's* means of complying with the requirements in *CASS* 17.4.4R to *CASS* 17.4.6R and *CASS* 17.4.8R to *CASS* 17.4.10R in clear and non-technical terms	Not specified	5 years after the version has been superseded by a new version
CASS 17.5.4R(3)	Each version of a *firm's* reconciliations policy document and reconciliations procedures document	The *firm's* rationale for its procedures to comply with the *rules* in *CASS* 17.5 in clear and non-technical terms, and those procedures	Not specified	5 years after the version has been superseded by a new version
CASS 17.5.9R	The *firm's per-trust/client/class cryptoasset requirement* and *per-trust/class cryptoasset resource*	The date and time, the actions taken and the outcome	Whenever the *firm* calculates a *per-trust/client/class cryptoasset requirement* or confirms a *per-trust/class cryptoasset resource*	5 years
CASS 17.5.10R(4)	*Client cryptoasset reconciliation record*	The date and time, whether there were any discrepancies and the reasons for them, and any actions taken	Each time a *firm* performs a *client cryptoasset reconciliation*	5 years
CASS 17.5.11R(2)	*Client cryptoasset discrepancy record*	The date and time, the reasons for the discrepancy and any actions taken	Each time a *firm* identifies a discrepancy outside of its processes for a	5 years

			client cryptoasset reconciliation	
CASS 17.6.10R	Each version of a *firm's* policy for the appointment of third parties under *CASS* 17.6	The *firm's* methodology for any selections, appointments, periodic reviews and consents that are required to be carried out under *CASS* 17.6.3R, *CASS* 17.6.5R and *CASS* 17.6.8R	Not specified	5 years after the version has been superseded by a new version
CASS 17.6.11R(1)	*Client cryptoasset third party due diligence record*	The grounds upon which the *firm's governing body* was satisfied of meeting the requirements of *CASS* 17.6.3R(1) to (4) or *CASS* 17.6.8R	Prior to the relevant appointment commencing	5 years after the relevant appointment ceases
CASS 17.6.11R(3)	*Client cryptoasset third party review record*	The conclusions of any periodic review performed under *CASS* 17.6.5R	The date the *firm* completes the review	5 years after the relevant appointment ceases
CASS 17.6.11R(5)	*Client cryptoasset third party governance record*	A *firm's governing body's* or its *governing body's* delegate's approval under *CASS* 17.6.9R(3)	The date of the *governing body's* or the *governing body's* delegate's approval	5 years after the relevant appointment ceases
CASS 17.7.3R(1)	*Cryptoasset safeguarding arrangement record*	A record of *arranging cryptoasset safeguarding*	When the *firm arranges cryptoasset safeguarding*	5 years

Sch 2 Notification requirements

Sch 2.1 G

Handbook reference	Matter to be notified	Contents of notification	Trigger event	Time allowed
…				
CASS 16.6.9R(3)(b)	…	…	…	…
CASS 17.5.15R	Failure to address a shortfall as required by *CASS* 7.5.13R	The reasons and other details as set out at *CASS* 17.5.15R(2)	Failure to address a shortfall	Immediately
CASS 17.5.16R(1)	The *firm's* internal records relating to *safeguarding cryptoassets* being materially out of date, or materially inaccurate or invalid	The fact of this issue	The *firm's* internal records relating to *safeguarding cryptoassets* being materially out of date, or materially inaccurate or invalid	Without delay
CASS 17.5.16R(2)	The *firm* being unable, or materially failing, to comply with *CASS* 17.5.6R, *CASS* 17.5.7R or *CASS* 17.5.10R	The fact of this issue	The *firm* being unable, or materially failing, to comply with *CASS* 17.5.6R, *CASS* 17.5.7R or *CASS* 17.5.10R	Without delay

…

Sch 5 Rights of actions for damages

…

Sch 5.2 G

		Paragraph	Right of action under Section 138D

Chapter / Appendix	Section / Annex		For private person?	Removed?	For other person?	
All *rules* in *CASS* with the status letter "E"			No	No	No	
All other *rules* in *CASS*, except *CASS* 6.4.1BAR(2)(c) ~~and~~, *CASS* 7.11.32R(2), *CASS* 17.1.6R(1), *CASS* 17.3.11R(2), *CASS* 17.6.3R(1)(c) and *CASS* 17.6.8R(2)(c).			Yes	No (except under *CASS* 6.4.1BBR ~~and~~, *CASS* 7.11.32AR, *CASS* 17.1.6R(2), *CASS* 17.3.11R(6), *CASS* 17.6.3R(2) and *CASS* 17.6.8R(5))	No	