APP Scams steering group - Draft Contingent Reimbursement Model Code

Response from the Building Societies Association

Restricted
09 November 2018

Building Societies Association

Set out below is the response from the Building Societies Association (BSA) to the draft APP Fraud Contingent Reimbursement Model Code and accompanying consultation published in September 2018 by the APP Scams Steering group / Contingent Reimbursement Model (CRM) Working Party.

The Building Societies Association (BSA) represents all 43 UK building societies. Building societies have total assets of over £396 billion and, together with their subsidiaries, hold residential mortgages of over £312 billion, 23% of the total outstanding in the UK. They hold over £276 billion of retail deposits, accounting for 18% of all such deposits in the UK. Building societies account for 37% of all cash ISA balances. They employ approximately 40,000 full and part-time staff and operate through approximately 1,550 branches.

Summary

- The objectives behind the draft CRM Code are sensible and desirable and have the building society sector's full support. Authorised push payment fraud (APP fraud) is a significant threat to consumers, firms and confidence in UK financial services that all stakeholders must work together to minimise.
- However, the Code's objectives have already been undermined by a dislocation between APP fraud policy and APP fraud infrastructure development that will create a 2 tier APP fraud protection environment for UK banks, building societies and their customers:
    - Tier 1 will consist of firms with full access to Confirmation of Payee from its implementation and full access to the infrastructure supporting the UK Finance APP fraud best practice principles.
    - Tier 2 will be those building societies, challenger banks and credit unions that will not have this access. Their customers (c.6.5 million building society customers) will be less well-protected against APP fraud.
    - Providing the wider infrastructure that tier 2 firms need access to in order to comply with the code is not a feasible option in the short term.
    - Tier 2 firms will be more likely to be targeted by criminals for laundering the proceeds of APP fraud once it is clear that they have fewer defences than tier 1 firms. The firms also still carry the reputational risk of public expectation to provide the same level of protection as tier 1 firms.
    - 2 tier APP fraud protection will also have consequences for the Financial Ombudsman service in determining what is fair in APP fraud complaints.
- This is obviously not what the Code intends but tier 2 firms would be immediately non-compliant through no fault of their own if they signed up to the CRM code in current form. There is a significant risk of a large number of tier 2 firms not signing up to the Code because of their disadvantaged position (and a public explanation of why they did not sign up) undermining the launch of the Code as an effective solution to tackling APP fraud.
- The dislocation between policy and infrastructure development that has led to the situation of two tier APP fraud protection is due to the absence of representatives of firms outside of the clearing banks on the CRM Working Group and related APP fraud prevention infrastructure development programmes.

- We strongly recommend that this state of affairs is addressed for the next stage of development and would like the Payment services regulator to take the lead in re-balancing representation.
- The APP Scams Steering Group needs to undertake an urgent review as to how the code can be adapted to operate within this unintended environment. The BSA and BSA members commit to working with the Steering Group and other APP fraud prevention programmes to make the CRM Code workable under the two tier APP fraud protection environment that consumers and firms will have to live with.

The position of building societies

As the code and related infrastructure delivery plans stand at the moment, most building societies would find themselves as tier 2 firms in terms of the APP fraud protection they can offer c.6.5 million customers.

Building societies certainly fit the target profile for the CRM code of "firms involved in making or receiving APP-associated payments between UK bank accounts who have control over preventing and responding to APP scams" and their customers are already being targeted for APP fraud. Our sector fully supports the objectives of the contingent reimbursement model to reduce the occurrence of APP fraud, increase customer-protection from the impact of APP fraud and minimise disruption to legitimate payment journeys. BSA Members will commit to adopting the CRM code's requirements in respect of fraud education, targeted fraud warnings and supporting fraud victims as best practice for their products and services.

However, the majority of building societies have a banking model that differs from that of a full payment services provider:

- They have no direct access to CHAPS, SWIFT and Faster Payments and use a clearing bank providing agency banking services to undertake transfers to other banks from their customers' accounts on their behalf.
- Some societies do allow transfers from internet–based savings accounts to the customer's current account but that account has to be nominated in advance and cannot be varied by the customer.
- Under current plans, firms using this banking model would not have access to the UK Finance-provided portal to report APP fraud to receiving banks or be able to offer their customers the Confirmation of Payee check – both are prerequisites for compliance with the proposed code.

Our members are considering carefully whether they should sign up for a voluntary code that they will be unable to implement in full. They are mindful of significant concerns about the customer service and reputational implications of not signing up – it is unlikely that consumer groups and other advocates of the code will be interested in reasons why some firms have to offer a lower level of APP fraud protection. They are also conscious of the implications for consumer confidence of the new code failing to meet its objectives at launch.

The position that the majority of BSA members now find themselves in is best summarised by feedback on this consultation from a BSA member:

"We along with other Building Societies are at an immediate disadvantage compared to larger banking organisations because:

- *Currently we are unable to fully participate with the Best Practice Standards as we do not have access to the UK Finance online portal (and therefore contacts) to submit APP fraud orders to the receiving banks*
- *As we do not have access to the portal we cannot receive the APP fraud notifications from the victim bank - UK Finance need to enable smaller organisations access to this facility to enable full participation.*
- *At this time, as a Building Society requiring a clearing bank, we are unaware whether we will be able to participate with the Confirmation of the Payee facility.*

We are prepared to re-evaluate our position as and when further clarification to the above points are released and we are able to fully participate with the Best Practice Standards and Confirmation of the Payee."

Current misalignment of policy and infrastructure

UK Finance online portal

Currently, access to the UK Finance online portal for reporting APP fraud to a receiving bank is only available for a certain level of UK Finance membership, which is above the needs of most BSA members who are also UK Finance members. It is not open to non-UK finances member such as BSA members who do not also have UK Finance membership. The result is that 41 out of 43 building societies currently do not have access to this portal and therefore could not fulfil their obligations under the proposed CRM code in full.

There is no suggestion that UK Finance have engineered this situation deliberately or that their intention is to act anti-competitively or leverage access to this portal to increase membership revenue.

The BSA is engaged with UK Finance on providing this wider access but there are significant development issues to sort out in respect of providing controlled access to their member-only website for non-members, building capacity for the portal to handle the extra capacity and the business case for this development compared to other development requirements on the UK Finance website. As of now, it is not possible to give guarantees as to when wider access will be available.

Confirmation of Payee

Confirmation of Payee is a banking infrastructure project running alongside but not co-ordinated with the CRM Working Party. Its target is that all payment service providers that are participants in Faster Payments be capable of sending confirmation of payee requests and presenting the response showing the name of the account that the payment is to be made to. their customers by July 2019.

For July 2019, "Customers" – will not include agency banking customers such as building societies and there is no commitment to provide Confirmation of Payee to them other than a vague intention to address this in a "phase 2". We hope that imminent consultation by the PSR on Confirmation of Payee will provide fuller commitment.

Delivering Confirmation of Payee is a significant technical development programme and - even if the promise of delivery in phase 2 was confirmed - it will be some time before banks could put this facility in place for building societies and other agency customers. However, it is important that the needs of agency banking customers are locked into Confirmation of Payee delivery now.

Development going forward

The CRM Working Group needs to undertake an urgent review as to how the CRM code can be adapted to operate within an (unintended) two tier APP fraud protection environment – as the code is written now it would be impossible for tier 2 firms to be able to comply.

The dislocation between policy and infrastructure development that has led to the situation of two tier APP fraud protection has been created by a lack of consideration of the role of banks and building societies outside of the major clearing banks in preventing APP fraud created by the absence of representatives of firms outside of the clearing banks on the CRM Working Group and related APP fraud prevention infrastructure development programmes.

We strongly recommend that this state of affairs is addressed for the next stage of development, led by the Payment Services Regulator.

The BSA and its members will commit to working closely the CRM Working Group and other programmes from now on - if invited to do so - to make sure that the CRM Code is made workable for the two tier APP fraud protection environment that firms and consumers will have to live with and to close the infrastructure gap between the two tiers.

Other aspects of the draft CRM Code:

- We support general duties for firms to provide fraud education, targeted warning and victim-support for customers. BSA members will commit to adopting these as best practice in their products and services.
- We also support the proposed duties for customers and firms where firms have the necessary capability to comply – though it may be helpful for customers to understand their duties in respect of APP fraud if they were written in plainer, less legalistic language with examples provided.
- The Code's current approach to vulnerability is too wide and may have unintended consequences. In particular, the Code's proposed introduction of assessments for vulnerability to fraud risks undermines one of the basic principles of supporting consumer vulnerability in that you support customers in vulnerable circumstances without judging how they got there. Case by case assessment of whether individual victims had vulnerable circumstances which would entitle them to automatic reimbursement will make maintaining that customer's trust and willingness to highlight difficult personal circumstances much more difficult by introducing a judgemental element around their circumstances.
- We agree with the working group's position on reimbursement for no fault cases that this is a good objective in principle but there will need to be a sustainable source of funding in place back up the principle with available funds before it can be delivered on. Our preference on funding would be a contribution mechanism across all parties with an ability to prevent APP scams from occurring including 3rd parties outside of

financial services, including redirection of fines by the ICO and other regulators for data loss, control weaknesses, failed cyber defences etc. which have led to APP fraud and recovered proceeds of crime from APP fraud.

- The Payment Services Regulator is the body most appropriate to take on supervision of / accountability for the Code and associated programmes.

Our responses to the questions highlighted in the consultation

What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?

Were the Code to achieve its stated objectives, UK consumers would benefit from a significant number of consumers targeted for APP fraud not becoming fraud victims and from the safety net of reimbursement of their losses in appropriate circumstances. However, we have concerns that the Code, as it stands, could inadvertently contribute to more fraud, more fraud victims, 2 tier APP fraud protection and undermine support for customers in vulnerable circumstances:

Investigation and prosecution of fraud – A likely consequence of introducing more frequent reimbursement so that fraud becomes a victimless crime is that APP fraud and other fraud will rapidly become de-prioritised by UK law enforcement when allocating already tight resources. A lower priority on fraud would be a signal to criminals that the UK is not taking fraud investigation and prosecution seriously and would lead to even more fraud being targeted at UK plc and UK consumers.

Consumer recklessness– Responses to the PSR consultation earlier in 2018 that created the working party highlighted significant concerns that the reimbursement safety net might lead to consumers becoming reckless about APP fraud risk knowing that they have the strong possibility of not suffering any loss if they have misjudged a fraudster's approach. We note that the current consultation does not address this behaviour and the risk remains. This could be dealt with by evidential standards requiring the customer to show that they were not reckless though the judgement culture that this would create would not be helpful for building consumers' trust in financial services – particularly vulnerable customers (see below).

Support for vulnerabilities - The Code's proposed introduction of assessments for vulnerability to fraud risks undermines one of the basic principles of supporting consumer vulnerability in that you support customers in vulnerable circumstances without judging how they got there. We understand the need to introduce a case by case assessment of whether individual victims had vulnerable circumstances which would entitle them to automatic reimbursement because there will be individuals who abuse this but this process will make maintaining that customer's trust and willingness to highlight difficult personal circumstances much more difficult by introducing a judgemental element around their circumstances.

Inconsistent application - So long as all institutions and customer comply with the Code and work the same, there should be no negative impact to the victims. There would be implications for consumers where the customer or institutions are difficult or incorporative. Each institution will have additional controls, reporting and training to implement.

Our most urgent concern is that customers of firms (and firms themselves) in tier 2 for access to fraud prevention and response measures would obviously suffer the risk of being less protected by the Code. – see below.

What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed? Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?

In its current state, the CRM Code and associated planned APP fraud prevention and response measures will create a 2 tier APP fraud protection environment for UK banks, building societies and their customers:

- Tier 1 will consist of firms with full access to Confirmation of Payee from its implementation and full access to the infrastructure supporting the UK Finance APP fraud best practice principles.
- Tier 2 will be those banks, building societies and credit unions that will not have this access. Their customers will be less well-protected against APP fraud.
- Tier 2 firms will be more likely to be targeted by criminals for laundering the proceeds of APP fraud once it is clear that they have fewer defences than tier 1 firms. The firms also still carry the reputational risk of being expected to provide the same level of protection as tier 1 firms.
- 2 tier APP fraud protection will also have consequences for the Financial Ombudsman service in determining what is fair in APP fraud complaints. It is unfair to penalise either the customer or a tier 2 firm in this unsatisfactory situation.

This is obviously not what the Code intends but we are currently in a position where a group of firms would face the consequences of non-compliance through no fault of their own if they signed up - as providing the wider infrastructure that tier 2 firms need access to is mandatory for compliance with the Code but not a feasible option in the short term.

There is a significant risk of a large number of tier 2 firms not signing up to the Code because of their disadvantaged position (and a public explanation of why they did not sign up) undermining the launch of the code as an effective solution to tackling APP fraud.

The APP Scams Steering Group needs to undertake an urgent review as to how the Code can be adapted to operate within this unintended environment.

We assume that none of the above were intended. Our observation is that this situation has occurred because of a lack of consideration of the role of banks and building societies outside of the major clearing banks in preventing APP fraud and a lack of understanding of the importance of wide availability of key parts of the infrastructure to deliver the code – for example Confirmation of Payee. This has led to dislocation between policy and infrastructure development. Lack of representation of firms who are outside the larger clearing banks as participants in the APP Scams Steering Group has not helped with encouraging a wider industry perspective.

The BSA and BSA members will commit to working closely with APP Scams Steering Group and other relevant APP fraud programmes from now on - if invited to do so - to make sure that the CRM code covers all banks and building society customers at risk of APP fraud effectively and consistently.

How should the effectiveness of the Code be measured?

Effectiveness should be measured on delivery of the steering group's draft principles as set out in this consultation. On those terms, the code would be considered to be effective if:

- The overall level of successful APP fraud falls.
- More APP fraud victims are suitably protected from the consequences of being a victim of APP fraud.
- More consumers are aware of the nature of APP fraud and what they can do to avoid becoming victims
- Where reimbursement is appropriate, victims receive reimbursement within agreed timescales.
- All firms have access to prevention and response measures so can fully adhere to the code.
- Evidential standards prove to be realistic and workable.

It would be ineffective if:

- The level of successful APP fraud continues to rise. In particular, if numbers of repeat fraud victims increases.
- Some building societies and banks are unable to adhere fully to the code through lack of access to underpinning infrastructure.
- The code itself becomes an MO for fraud.
- The pressure for both firms and victims to prove that evidential standards have been met makes the customer relationship more adversarial and introduces a judgemental approach to customer vulnerability.

Effectiveness could also be assess through complaint numbers (the more complaints the less the code is working); focus groups and feedback from trade bodies.

Do you agree with the standards set out in the Standards for Firms?

We broadly agree with the standards set for firms, with the following qualifications reflecting the different levels of access to the infrastructure underpinning the Code and circumstances of a current account provider and a savings account provider:

SF1, (1), a – Firms who offer savings products only will not have the same granularity of transaction data that current account providers have so customer behaviour analytics will be less effective in identifying payments that are at higher risk of APP fraud.

SF1, (3) & SF2 (2) – There is no certainty when Confirmation of Payee will be available to building societies and smaller banks who rely on an agency bank to provide money transmission services to their customers.

SF1, (6) & SF2, (4) – Notifying receiving firms when an APP fraud is reported using the UK Finance best practice standard requires access to the relevant UK Finance Portal. At present access is only available to full members of UK Finance, which means that 41 of 43 building societies (credit unions also) do not have access to this facility and so would be unable to comply with this requirement.

The implications for firms not meeting these standards need to be reconsidered for those firms who don't have access to the APP fraud prevention infrastructure required for compliance with the above.

We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims. We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

Our members feel that a level playing field is required so that the customer cannot claim off both institutions. It would be useful to have central contacts so that firms can discuss common cases.

We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

Under current plans for the roll out of Confirmation of Payee it is not known when every firm will have Confirmation of Payee capability - the provision R2(1)b should not apply where the firm has not been given that capability.

We find it hard to envision a scenario where a firm has failed to provide an effective warning and the customer has then failed to act on it. The customer can't fail to act on a warning that hasn't been made. Our members suggest that it would be useful to have some examples of when this could apply. The Society feels where evidence shows all parties have not met the level of care, a 3 way split could be applied.

We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

Under current plans for the roll out of Confirmation of Payee it is not known when every firm will have Confirmation of payee capability - the provision R2(1)b should not apply where the firm has not been given that capability.

We find it hard to envision a scenario where a firm has failed to provide an effective warning and the customer has then failed to act on it. The customer can't fail to act on a warning that hasn't been made.

Do you agree with the steps customers should take to protect themselves?

We agree that the customer should take responsibility for failure to spot APP fraud when they have received clear warnings or advice that they are at risk on a particular transaction. We propose amending the list of warnings in R2(1) to include:

- Warning given by the firm's staff at a branch counter or by telephone

- Warnings given to the customer by 3rd parties with whom the customer has a relationship who had warned the customer that they had been victims to cyber attack, data loss etc. and so the customer was at risk of fraudsters using their name.

Feedback from members is that with each case, the whole scenario needs to be reviewed. For example, where firms have provided a high amount of information and education to customers about these scams, the customer should bear some of the responsibility. Vulnerable customers should also be treated carefully and be made aware when they might have been scammed for their protection

As an observation, much of the language used in this section of the Code is very legalistic – for example "recklessly sharing access ", "failure to take reasonable steps" and "not acted openly and honestly". It would be helpful to both customers and firms to set out the customer's duty to protect themselves in plainer language and to include case study examples of what these terms mean.

Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

We strongly support the principle that a customer in vulnerable circumstances who is less able to protect themselves against APP fraud in the manner outlined in section R2 of the Code should not be barred from receiving reimbursement because of those circumstances. We also agree that it is right for firms to have to assess cases individually and solely in the context of vulnerability to a particular incident of APP fraud. However, there is concern that vulnerability is being applied too widely:

- Where customers are repeat victims of APP fraud, where do you draw the line between vulnerability and recklessness – not all types of vulnerable circumstances justify a customer not following warnings or past experience?
- What is the relevance of vulnerability in cases where the customer is acting logically and responsibly by responding to a legitimate request to pay monies due to a known third party that are then diverted by fraudsters?
- Requiring firms to reimburse customers whether or not the firm knew of their particular vulnerable circumstances at the time is not an approach that is fair to both the firm and the customer and has the potential to open firms to claims of retrospective consumer vulnerability by individuals, unscrupulous families or claims management companies.
- Assessing the non-financial impact of an APP fraud on a particular fraud victim requires financial services firms to act as medical experts - which is an inappropriate requirement on these employees.

In terms of unintended consequences, our major concern is that this approach pushes firms to become more intrusive and interventionist with their customers and to assess vulnerability on a judgemental and legalistic basis and make value judgements on how they think the customer should have behaved. For example, the test of whether it would be "reasonable to expect the customer to have protected themselves, at the time of becoming a victim of an APP fraud,

against that particular APP fraud to the extent of the impact they suffered" is difficult to assess without an intrusive review of the customer's personal circumstance and their handling of the payment journey.

This is a significant move away from the basics of good customer support as highlighted in the FCA's Occasional Paper *"Consumer vulnerability"* and other codes of practice where an environment where customers with problems feel comfortable about raising them without being judged on how they came to be there is key. There will be severe pressure on trust between firms and customers in circumstances where keeping the customers' trust is key to supporting them through them.

Do you agree with the timeframe for notifying customers on the reimbursement decision?

We believe this proposal to be reasonable but the timeframe should be kept under review to ensure that it fits with real life administration of the Code. Members feel that the customer must also report the scam in a reasonable timeframe and that there should be a maximum period of which the customer must report the fraud by. The customer must respond to any requests for additional information promptly.

Please provide feedback on the measures and tools in this Annex, and whether there any other measures or tools that should be included?

As we have previously noted we are concerned that not every building society or bank has access to Confirmation of Payee and the infrastructure required for best practice standards for responding to APP fraud – which makes them vulnerable to being particularly targeted for fraud and at a competitive disadvantage in offering fraud protection against those who do. We suspect that there will be a similar disparity of access for Network-level transaction data analytics and Economic crime information sharing.

We would like confirmation of plans to ensure appropriate access for all firms to all of the fraud prevention and response tools outlined within the Annex to the Code.

Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?

We agree in principle – though this premise needs to be kept under review for evidence that this is making customers reckless to fraud risk. We also support the position taken in this consultation that there will need to be a sustainable pool of funding for no fault reimbursement to back up the principle with available funds before it can be delivered on.

It also needs to be clear to consumers that reimbursement under the Code is for monies lost to fraudsters only – falling victim to high-pressure sales tactics from legitimate firms, unwise spending decisions and buyer / seller disputes are not APP fraud and there should be no entitlement to reimbursement from funds reserved for APP fraud reimbursement in these circumstances.

Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

We agree that the sending bank should not be directly liable for the cost of no fault reimbursement if it has met its own standard of care – though the above statement does imply that the sending bank has some indirect liability. We would like clarification on what the consultation's authors believe any indirect liability to be.

We also agree for the sake of simplicity and delivering a quick outcome for the customer that the sending firm should administer any no fault reimbursement where the transfer is between two Payment Services providers (PSPs,) subject to confirmation of the source of funding for these payments. However, in the building society context, this is not the usual chain of events - most building societies and smaller banks provide facilities for CHAPS transfers from a customer's savings account to a 3rd party's account with the CHAPS transfer being administered by the society's own bank. In this scenario,

In these circumstances, we would like confirmation of who should be treated as the "sending firm" - the building society where the transferred funds were taken from or the bank that provided the CHAPS facilities to make the transfer?

What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?

Any funding model must take into account that PSPs and customers are not always the only parties to an APP fraud and sometimes 3rd parties can enable the fraud to take place through their failure or negligence. Often, action or lack of action by a non-bank third party is the key to the fraudster's ability to convince the customer to authorise the fraud and they should face primary liability for compensating their customer (the PSR used an example of a firm of solicitors whose lax cyber-defences created the opportunity for APP fraud).

In such cases, it should not be the role of the financial services industry to subsidise failure in other sectors nor will regulators' objective of incentivising better anti-fraud practice in future be met if non-bank parties do not have the same incentives as PSPs to improve poor anti-crime defences.

Therefore, our preference would be a contribution mechanism across all parties with an ability to prevent APP scams from occurring (option a), including redirection of fines by the ICO and other regulators for data loss, control weaknesses, failed cyber defences etc. that enabled fraud. We would also advocate diversion of recovered proceeds of crime from APP fraud to contribute to funding "no fault" reimbursement, particularly where the affected fraud victims have already been compensated under the APP Code arrangements. Fines to banks in shared blame scenarios (option e) could also feed into this fund – but only if the Code was re-drafted to account for two tier APP fraud protection.

How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?

As discussed previously, we are concerned that use of evidential standards for firms and consumers – particularly in respect of vulnerability will pushes firms to become more intrusive and interventionist with their customers and to have to assess their conduct on a judgemental and legalistic basis that will make the future customer relationship much more difficult. Plainer, less legalistic language might help make this process less intimidating for both parties.

Do you agree with the issues the evidential approach working group will consider?

We agree – particularly with the objective that evidential standards should be reasonable and fair to all parties involved in the scam.

Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

As (unintended) two tier APP fraud protection is going to be a with us for some time, the Evidential Approach working group will have to consider the issue of different evidential standards for tier 2 firms so that their requisite level of care aligns with their lack of access to APP fraud prevention infrastructure.

Members also recommend that the payee firm evidences any CDD taken. There should also be evidence in regards any ongoing payments to further institutions.

How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

All assessment of vulnerability in the context of vulnerability to an APP fraud should treated as the customer's sensitive personal data and be conducted and recorded according to the consumer privacy requirements of the General Data Protection Regulation.

There does need to be a debate on how much of the information collected is shared with other institutions subsequently – for example aggregation services and open banking product providers – though this is not an issue just for APP fraud.

Please provide views on which body would be appropriate to govern the code.

The Payment Services Regulator (PSR) would be the most appropriate body to govern the code, given its existing position as a regulator and statutory objectives.

- The current dislocation between policy and infrastructure delivery for APP fraud prevention appears to have occurred because there was no effective central body overseeing APP fraud prevention development in the round – this situation needs to be remedied from now on. The PSR with its objective "to ensure that payment systems are operated and developed in a way that considers and promotes the interests of all the businesses and consumers that use them" is the natural body to take on formal responsibility for proper co-ordination of policy and infrastructure.
- The complexity of the evidential and dispute resolution arrangements that the code will need to have in place means that a regulator's authority is needed to oversee the mechanisms behind the code.
- The code needs a governing body with sufficient authority to deliver a level playing field of access to fraud prevention / response tools.
- As the code touches on two very significant public policy issues in financial crime and consumer protection it is important that the overseeing body has clear accountability to the supervisory authorities for the UK economy and to Parliament - which the PSR already has.
- The PSR is already established so there would be no additional set up costs required.

We agree that it would be inappropriate for UK Finance to become the Code's governing body as there is a potential conflict of interest with their core role of promoting the interest of its members. For the same reason, creating a governing body out of the membership of the working group would also be inappropriate because many of the groups involved are also advocates for a particular agenda or interest group. There is no conflict of interest in the PSR assuming this role.

Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

A 50:50 apportionment of reimbursement between two PSPs at fault is a reasonable start point position in terms of simplicity and a quicker result for the fraud victim But, this should be kept under review.

Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the Code? What issues or risks do we need to consider when designing a dispute mechanism?

Our members believe these principles are appropriate – subject to being adapted to handle two tier APP fraud protection. However, as regards Open Banking itself, there are some concerns: How easy would this information be access; would it be by a fee; would it be by a 3rd party provider (e.g. CIFAS, not all institutions are members of); who would be to blame if the information was hacked or the system was down?

Other questions and comments on this consultation from BSA members

Section 4.8: Once the mechanism is created, there will need to be a process in place to reassess the ongoing funding, based on the amount remaining and the reimbursement decisions made. It is likely, therefore, that the contribution levels would change periodically and we would hope that they would reduce over time as the improved levels of care reduce APP scams. How would a small firm budget for these regular changes in costs and possible changes?

Section 4.9: *Until a funding mechanism is identified, customers might not be reimbursed in the scenario where all parties have net their expected level of care under the code. Once the funding mechanism has been agreed, whether it is legally and practically possible for customers to claim from that mechanism for 'no blame' cases occurring during the consultation period will be considered. However, this may result in 'no-blame' victims of APP scams occurring during the consultation period not receiving reimbursement.* Will this result in customers – possibly assisted by CMCs - complaining and reopening old cases which were addressed before the code?

Table 2 in Annex – *Credit Flags: Individuals can be registered as not having capacity and a flag placed on their account. With this flag, if credit is applied for in their name, it will be refused and a notification delivered to the person who registered the individual.* How will banks share this information? Is this compliant under GDPR?

Table 3 in Annex – *Current practice on APP fraud statistics. App fraud statistics ae collected and provided on a monthly basis to UK Finance who in turn, publishes these on a 6 monthly basis.* No all firms are UK Finance members. There is the possibility of double reporting where the fraud involved a transfer of funds from a savings account to a current account before the final payment to the fraudster.

Other - What will be the timescales the customer has to report the fraud by? We suggest 24 hours. What is to happen if they reported it 12 months later? This would be unrealistic for a firm to investigate.

What if the customer has just forgotten what they paid for or what if it is a dispute between the customer and the payee?

How will reimbursement happen; would it be different for each institution? If an invoice is sent, how quickly is this to be paid? What happens if one institution claims to have lost it after being chased? There may be difficulties in making firms pay their share.

If one institution is slow at responding to queries or lose information, what are the next steps which can take place by the other institution who have the victim waiting?

By James O'Sullivan
Policy Adviser
james.osullivan@bsa.org.uk
0207 520 5916

York House
23 Kingsway
London WC2B 6UJ

020 7520 5900
@BSABuildingSocs
www.bsa.org.uk

BSA EU Transparency Register No: 924933110421-64

www.bsa.org.uk

The Building Societies Association (BSA) is the voice of the UK's building societies and also represents a number of credit unions.

We fulfil two key roles. We provide our members with information to help them run their businesses. We also represent their interests to audiences including the Financial Conduct Authority, Prudential Regulation Authority and other regulators, the Government and Parliament, the Bank of England, the media and other opinion formers, and the general public.

Our members have total assets of over £387 billion, and account for 22% of the UK mortgage market and 18% of the UK savings market.