Building Societies Association – Written evidence (FDF0023)

Executive Summary

The Building Societies Association (BSA) represents all 43 UK building societies, as well as six large credit unions. The key points in our submission are:

- Authorised Push Payment (APP) fraud is the fastest growing type of fraud for building society customers – though the volume of building society APP fraud cases is significantly lower than for retail banks. (1)
- Fraud as a crime is not treated with the priority that its frequency and impact on victims deserves. (9)
- All parties that provide services that could be misused by fraudsters or which could be adapted into fraud scams have a shared responsibility to protect the public against all forms of fraud. (14)
- Unfortunately, the payments system-based approach to fraud prevention has created a two tier fraud prevention infrastructure. Some payment services providers, such as building societies, were left out of the development of the Contingent Reimbursement Model (CRM) Code and Confirmation of Payee because system designers focused solely on current accounts. (17)
- The one policy recommendation that the BSA and our members would ask the Committee to make to the Government would be to consider very carefully the full consequences of making APP fraud a victimless crime before proposals to introduce mandatory reimbursement of APP fraud victims are followed through. (33)
- We have no problem with the concept of building societies/banks reimbursing APP fraud losses where they contributed to the execution of the fraud. (34)
- We recommend that there is an in-depth analysis and debate on the full consequences of any proposals to make APP fraud a victimless crime. This should also consider whether there are alternatives that would deliver lower numbers of fraud victims, as well as providing an appropriate compensation safety net. (35)

Fraud Landscape

What fraud risks are UK a) individuals, b) the Government and c) businesses particularly vulnerable to today, and what are the reasons for this?

Individuals

1. Table 1 sets out the common types of fraud targeted against building society customers. Across the UK as a whole, APP fraud is the fastest growing type of fraud in the UK by both volume and value, followed by card fraud. However, given the limited savings/mortgage product range that building societies provide and the sector's customer demographic APP fraud is significantly lower within the sector and frauds associated with exploiting vulnerabilities relatively high. The exception is Nationwide

Building Society which, as a full service current account provider, has similar APP fraud levels to its retail bank peers.

Table 1: Common types of fraud targeted against building society customers

FRAUD TYPE	HOW IT WORKS	EXAMPLES
Authorised Push Payment (APP) Fraud	Customer is tricked into authorising payments to a scam or giving fraudsters access to their account	Investment fraud Phishing & Vishing Online shopping scams Safe account scams Diversion of payments fraud Ponzi schemes Bogus official penalty scams Advance fee fraud
First party fraud	Building society is tricked into authoring a withdrawal from a customer's account / advancing credit without their authority.	Forged signatures Cheque fraud Mortgage fraud
Fraud associated with exploiting vulnerabilities	Fraudster exploits their victim's vulnerabilities to obtain money by fraud.	Romance scams Postal scams Rogue traders Fraud by abuse of position
Impersonation/ account takeover fraud	Fraudster uses knowledge of victim's financial affairs to take over their accounts	First party fraud Credit application fraud
Card fraud	Unauthorised use of credit / debit / ATM cards	Card purchase fraud Card skimming

2. Common characteristics for all fraud types are:

- Fraudsters' use of pressurised decision making to steer their victim away from questioning the context of the transaction either by the incentive of potential missed opportunity of by the threat of bogus sanction or unwanted outcomes if the victim does not comply.
- Impersonation of official bodies – HMRC, the police, government departments & agencies – to make the threat of non-compliance as realistic as possible.

- Investment in efforts to gain the victim's confidence often using personal information obtained from social media to support their false identity.
- Use of online channels and telecoms technology to maximise their reach, disguise their origins and obtain access to personal information.

Government

3. Fraudsters have the same opportunity to use similar techniques to commit fraud against government by targeting the balance that government has to maintain between providing financial support for individuals and business promptly and easily while also checking that they are properly entitled to receive it. The recent revelations on fraud associated with COVID support payments to business is a good example of how fraudsters profit from pressure on the government to act quickly. The most common fraud against government seen by building societies is benefits fraud – not just by individual claimants but also co-ordinated fraud run by organised crime.

BSA members

4. Unsurprisingly, mortgage fraud is a particular issue for BSA members. This can be divided into fraud for purchase – where mortgage applicants doctor their application forms to obtain a higher loan than they are entitled to leading to losses later on when they are unable to pay – and fraud for profit – where organised syndicates involving corrupt professionals in the house buying chain obtain loans on false pretences, which are never repaid. Mortgage fraud for purchase is a consistent problem for lenders but mortgage fraud for profit has reduced in recent years as organised crime has switched to simpler, more profitable APP frauds.
5. Like other companies, BSA members are also targeted by scams probing for weaknesses in their internal systems and controls such as payment diversion, invoice fraud and senior management impersonation fraud.

What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years, and how might these be prepared for and mitigated? What role can technology and tech companies play in combatting fraud across this timescale?

6. Fraudsters generally use a narrow range of scam scenarios that have evolved from face to face conversations to be adaptable to telephone, SMS email and online rather than inventing completely new scams to respond to developments in technology. They are particularly skilled at adapting these scenarios to events or economic circumstances to exploit consumers' preoccupations at any given time. The proliferation of COVID 19-related scams at the start of lockdown in the UK where fraudsters re-positioned existing scam modus operendi with a COVID context and the way that these scams were modified to match the pressures of continued lock-down as it continued is a good example of fraudsters' capability to adapt to circumstances. We do not expect this approach to change and would therefore expect to see an increase in fraud scams adapted to prey on concerns about the increasing cost of living in the UK and use of the

situation in Ukraine for bogus charity scams alongside more familiar types of scam.

7. Where technology has been of enormous benefit to fraudsters is that it creates the ability analyse social media and other channels holding personal information to target scams more effectively, to circulate mass-volume scams cheaply and easily while disguising the identity of the sender and to mimic legitimate websites and telephone numbers so that victims are deceived into a false sense of security. The internet has also made it possible for organised crime to share information / best practice and to trade consumers' personal data as a commodity. Again, we would expect all of the above to continue.

8. However, we do expect increasing application of technology to make fraud more difficult - for example personalised fraud warnings when consumers make certain transactions, the ability to pause payments to assess fraud risk and expanded use of biometrics to uniquely identify that the user of payment channel is a legitimate user. Tech companies will also have a key role in combatting fraud via consumer fraud education – particularly in the open banking environment where the customer's first point of contact for help will be a fintech company not a bank or building society. It is important that tech firms are fraud-conscious and that fraud risk is assessed and highlighted to consumers for all new future technologies as they develop.

Is fraud and its victims treated as a priority? If not, what are the reasons for this? The Committee is particularly interested in responses that can explain any barriers preventing effective counter-fraud cooperation within Government, law enforcement, the public sector and the private sector.

9. Fraud as a crime is not treated with the priority that its frequency and impact on victims deserves. BSA members and other financial services firms have had a long history of difficulty with law enforcement being willing to take on fraud investigations when cases are presented to them and this situation has not changed despite the very rapid growth of APP fraud cases in the last four years. Latest UK crime data showed a 36% increase in reported fraud offences and a 161% increase in unauthorised access to personal information (including hacking) offences in comparison to a 14% reduction in other types of crime from 2019 to 2021 (ONS Crime in England and Wales: year ending September 2021). There has been no consequent realignment of law enforcement resources to investigate more fraud.

10. The reasons for this are summarised in the 2019 HMICFRS (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services) report Fraud: Time to Choose - An inspection of the police response to fraud:

    - There is no national strategy for tackling fraud. Police forces have therefore developed a range of different responses. Across police forces, regional organised crime units and national bodies, there is no clear understanding of who is responsible for fraud-related activities or what the expected level of performance is.
    - Lack of capacity and capability within police fraud investigation teams

- Competing priorities – ""fraud does not bang, bleed, or shout" so has relatively low priority with chief constables and police and crime commissioners when making difficult decisions on allocation of resources.
- Typically, fraud investigations are relatively high cost and long term so there is a reluctance to take investigations / prosecutions forward, particularly where the investigation includes parties based outside of the UK.

11. The 2019 HMICFRS report concluded "while we understand why fraud may not be considered a priority for some (police) organisations, it does not follow that we accept that the current position should be allowed to prevail". Despite some progress in creating a national strategy for tacking fraud following the launch of the Economic Crime Strategic Board and the UK Economic Crime Plan we have seen no progress on raising the priority of fraud within law enforcement. But, we also agree with the HMICFRS report that, despite the above, there has been real progress in public-\ private sector co-operation on tacking fraud at ground level resulting in individuals targeted for scams stopped from becoming victims – examples include the Banking Protocol and the HMRC Mortgage Service. This suggests that the barriers to fraud being treated as a priority are not based on sectors failing to work together.

12. On victims of fraud, the HMICFRS report concluded that vulnerable victims generally receive good care and advice on how to protect themselves but that other victims are often given confusing and misleading advice about how (or whether) their case will be investigated and, if it is, how it is progressing. In the private sector, there has been much more focus on support for the victims of fraud particularly the expectation that "banks" should reimburse victims of APP fraud for losses incurred – which we take as a tacit acknowledgement that fraud victims are unlikely to have any losses recovered through action by UK law enforcement.

Action to Tackle Fraud

How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

13. The BSA and its members have no privileged access to performance data on the policing of fraud and so our observations are based on the HMICFRS report and on Fraud and cyber-crime national statistics data.

    - The HMICFRS report identified that City Of London Police should continue as lead force for fraud but needed to be more effectively held to account in relation to how it carries out these functions. In our experience, they are willing to engage and share their expertise with financial services trade bodies.
    - The National Fraud Intelligence Bureau (NFIB) is a valuable source of financial crime alerts to our members. The HMICFRS report commented that NFIB provided police forces with good quality fraud intelligence products but how police forces followed them up was inconsistent and sometimes ineffectual.

- We are aware that ActionFraud has been severely criticised for its repeated poor service to consumers and that the UK Economic Crime Plan contains plans for its closure and replacement by a new organisation.

What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?

14. All parties that provide services that could be misused by fraudsters or which could be adapted into fraud scams have a shared responsibility to protect the public against all forms of fraud. This includes government, local government, public bodies and charities as well as the private sector. Protecting the public requires:

    - Supporting fraud awareness education for consumers and businesses via fraud both general awareness campaigns and specific warnings about particular scams targeted at their clientele.
    - Supporting the investigation and prosecution of fraud
    - Supporting individuals targeted for fraud – ideally by preventing them becoming victims.

15. Digital fraud is no different in this respect – any providers of digital services that could be targeted by fraudsters (public or private sector) should have the same responsibility to protect the public. We do accept that building societies, banks and other payment service providers have a particular responsibility to protect their customers from fraud by virtue of providing access to the payment systems that would be used to make payments to a fraudster (now confirmed by the recent Court of Appeal judgement in Phipps vs Barclays Bank UK) and our members have invested significantly in suitable fraud controls to match the digital services that they offer. But other sectors within the digital infrastructure, such as telecoms and social media, are also well-positioned to intervene to stop fraud. All organisations whose names fraudsters take in vain to authenticate fraud scams – including public sector bodies such as HMRC - also have a responsibility to alert users of their services to potential fraud.

16. In terms of balance, the most effective approach is to build fraud awareness into service development so that all new / improved services come with suitable fraud protection measures deployed alongside and potential users are prepared for potential fraud early on. This is particularly important in the context of digital services as system-specialist designers and developers do not always acknowledge non-system risks (regulators and payments industry bodies included). A good example of what can go wrong was the modifications to Faster Payments following the second EU Payments Directive. Implementation in the UK concentrated solely on delivering speed of transaction and chose to ignore risks that too much speed did not give time for customers to consider fraud risk or payment services providers to recover funds paid to fraudsters. This is now under review to assess the feasibility of building in "pause" technology but at a higher cost than incorporation from the beginning.

17. Unfortunately, the narrow, payments system-based approach is still prevalent in some quarters of financial services regulation and this has inadvertently created a two tier fraud prevention infrastructure where payment services provider such as building societies were left out of the development of the Contingent Reimbursement Model (CRM) Code and Confirmation of Payee because of system designers focusing solely on current accounts. Hard lobbying of the Payment Systems Regulator and Pay.UK has put our sector back onto the agenda for both but, as of now, BSA members cannot participate in either scheme.

What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

18. This is a particularly legally complicated area that needs to be addressed by cross-sector action led by the agency (i.e. government) that has the ability to deliver the changes required. We are pleased to see that the UK Economic Crime Plan contains a taskforce specifically to review both the legislative / regulatory and the practical barriers to sharing fraud data more widely and what is required to break them down.

19. There is a wider policy issue created by GDPR. Fraud data relating to victims is their personal data under GDPR and the Date Protection Act 2018 which gives fraud victims the right to veto wider circulation of their personal data. Organisations that want to share it more widely are required to ask first but which allows data on criminals or fraud suspects to be shared without this. More sharing of fraud victim data would help a range of organisations better protect victims individually and collectively but the dilemma is whether to widen the Data Protection Act exemption relating to preventing / investigating crime to include fraud victim data to enhance fraud protection as a whole at the price of affording the victim less data privacy rights and treating them in data protection terms as equivalent to a criminal suspect.

What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to prevent them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

20. The best defence against fraud is not to become a victim in the first place, so individual consumers' own knowledge and willingness to be suspicious about potential scams are the first line of defence against fraud. As providers of financial services, BSA members encourage their customers to take responsibility for guarding against fraud and for following up on suspicions of fraud, both their own instincts and information from others. But there are still consumers who appear not to learn from previous experience or to follow up on fraud warnings. Some do so because they have vulnerable circumstances that make them more likely to make poor decisions – for example fluctuating mental health / mental capacity or very low financial resilience or capability. But for others the root cause of poor decisions is often over-confidence or over-hastiness. It should also be remembered that fraudsters can be extremely persuasive and use replicated personal information, company registration and official phone numbers / websites to create a false sense of security for their victim so a

consumer could act with considerable prudence and still end up becoming a fraud victim.

21. We are strongly against any type of penalty or discrimination being applied to victims of fraud just because they have become a victim. One of the issues faced in tackling fraud is the perceived stigma of having fallen for a scam which prevents many consumers from reporting the scam or even sharing with others what happened and how they were duped – this is not helpful either to that consumer or to improving fraud education as a whole. However, it is reasonable to consider the consumers' actions or lack of actions in the context of reimbursement for APP fraud losses on a case by case basis as laid out in the CRM Code - though we also accept that inconsistent application of CRM Code requirements between current Code members has made things more difficult for fraud victims and that there is work to do to ensure that consumers can be confident of a consistent service.

22. In terms of consumer / business fraud education, all parties that provide services that could be misused by fraudsters or which could be adapted into fraud scams have a role to play as well as consumer groups and charities – again financial services firms have a particularly important role. Lots of organisations do provide valuable fraud education services for consumers in general or for particular groups of consumers – examples include the financial services industry's Take 5 to Stop Fraud campaign, UK Trading Standards' Friends against Scams and awareness campaigns by Which?, Age UK, Utilities against Scams and the National Union of Students for their particular constituencies. There is still opportunity to do more – in particular organisations who know that fraudsters use their names of scams could do more to raise awareness among their clientele.

23. Among the most effective methods of fraud education are real life examples and shared experiences passed on between consumers– hence the importance of tackling the stigma associated with becoming a victim of fraud. We would also like to see more follow-up analysis on successful fraud prevention interventions to analyse and share as best practice the messages / media that worked particularly well to make consumers avoid becoming fraud victims. Too often, we receive feedback on fraud education initiatives that focusses on why they did not work for particular types of consumers. While this is valuable it would be more effective to learn how / why successes were achieved.

Legislative Remedies

What is your assessment of the Fraud Act 2006? What has been the impact of the Act and is it having any unintended consequences; if so, what are these?

24. There have been recent high profile cases where attempted prosecutions for fraud have failed publicly for a range of reasons – the BSA is not best placed to assess whether this was due to problems with the Fraud Act or other problems with these prosecutions.

25. The barriers to successful prosecution of less complex, lower level fraud of the sort that BSA members and their customers face are not around construction of legislation but around a degree of unwillingness by police forces and prosecuting bodes to bring cases to prosecution.

Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions? Answers may refer to existing mechanisms such as increasing the scope and powers of regulators. You may refer to any legislation and are not limited to the Fraud Act 2006.

26. Please see answer above on the Fraud Act 2006.

27. We are pleased that the government has included measures against promotion of fraud scams within the Online Harms Bill. This is an important step in developing a joined-up regulatory environment for fraud to support the UK's Economic Crime Plan by addressing some fraud risks that are currently outside the perimeter of regulation by the FCA but involving authorised firms - as highlighted by the collapse of London Capital & Finance in 2021.

Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?

28. Please see answer above on the Fraud Act 2006.

Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful?

29. Current sanctions and penalties – including prison sentences and the forfeiture of proceeds of crime – do not appear to be an effective deterrent to fraudsters.

    - A typical sentence for a fraud offence is 2 years in prison – with the prospect of early release for good behaviour. Latest data on re-offending shows that 18% of adults and 38% of juvenile offenders in England and Wales convicted of fraud subsequently commit a proven fraud re-offence within 12 months of release from prison (Ministry of Justice Proven reoffending statistics: January to March 2020) suggesting that current prison sentences for convicted fraudsters are not effective deterrents.
    - Confiscation of the proceeds of crime is another potential deterrent The value of proceeds of crime recovered from Civil Recovery orders was £12.7m for the financial year 2020 to 2021 (ONS Asset recovery statistical bulletin, September 2021). While this represents a 42% increase from 2019/2020 it is still very low when set against fraud losses of c.£500m for the same period and strongly suggests that a fraudster will still be able to enjoy the profits of their crime post-conviction.

30. Longer prison sentences – particularly for criminals who specialise in fraud associated with exploiting vulnerabilities – plus more effective confiscation of the proceeds of fraud would be a greater deterrent. We would also support appropriate community-based sentences for fraud. However, changes to sentencing / penalties would only succeed in tandem with committing more law enforcement resources to investigating and prosecuting more fraud cases.

Best Practice

What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

31. From the BSA’s point of view the most successful recent fraud policy intervention has been the Banking Protocol. This private / public initiative involving UK police forces, building societies and banks gives building societies and banks the option to bring in guaranteed police intervention where there are concerns that a customer might be being targeted for fraud. It was launched in 2016 initially focussing on branch customers but now includes telephone and online banking. In the period 2016-2021 the scheme stopped fraud to the value of £142m and led to 900 arrests.

32. Lessons for future schemes include:

    - The Banking Protocol being a genuine partnership from its inception.
    - It is adaptable to cover a range of types of fraud plus a wide variety of banking products and channels so can equally be used by the big retail banks and smaller savings account providers.
    - Implementation started with a pilot within one London borough before national rollout so that all would be participants could clearly see the benefits of becoming involved.
    - The scheme’s progress is monitored by collecting management information to illustrate its performance.
    - The scheme has built on success and exchanges of best practice between participants.

Can you suggest one policy recommendation that the Committee should make to the Government?

33. The one policy recommendation that the BSA and our members would ask the Committee to make to the Government would be to consider very carefully the full consequences of making APP fraud a victimless crime before proposals to introduce mandatory reimbursement of APP fraud victims are followed through. This concern has been prompted by recommendations for the introduction of mandatory reimbursement of APP fraud victims included in the Payment Systems Regulator’s Authorised push payment (APP) scams, Consultation paper November 2021.

34. We have no problem with the concept of building societies / banks reimbursing APP fraud losses where they (the building society / bank) contributed to the execution of the fraud – this has long been the case for first party fraud and should be the same for APP fraud. We also recognise that the introduction of the CRM Code on APP fraud reimbursement has not been totally successful so we understand why the PSR is keen to move quickly to help more fraud victims of fraud get access to reimbursement. However, removing the risk element of APP fraud for consumers by mandatory reimbursement – making it effectively a victimless crime - creates a range of potential unintended consequences and it is worrying that PSR has presented its recommendations without any acknowledgement or consideration of issues such as:

- The impact on consumer behaviour if fraud risk is removed from transactions.
- Removal of incentives for law enforcement to tackle fraud.
- Removal of incentives for fraud-enabling sectors outside of retail banks and building societies to tackle fraud.
- Impact on UK legal framework for contract law – in particular, reconciling mandatory reimbursement with the Caveat Emptor principle.
- Likelihood of more not fewer fraud scams being targeted at the UK.
- The impact on wider crime if more funding from proceeds of fraud becomes available.

35. We recommend to the Committee and the Government that there is an in-depth analysis and debate on the full consequences of any proposals to make APP fraud a victimless crime via compulsory reimbursement for APP fraud victims. This should also consider whether there are alternatives that would deliver lower numbers of fraud victims, as well as providing an appropriate compensation safety net. The proposals would require a change in legislation to allow implementation, which should allow Government and Parliament the opportunity time for appropriate scrutiny.

21 April 2022