Sardine – Written evidence (SCG0047)

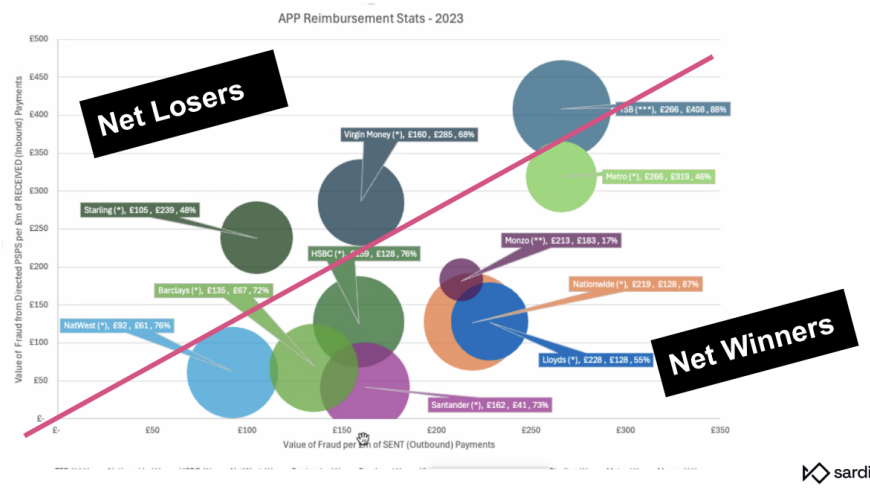
1. **In response to Lord Forsyth's question on the costs to firms associated with APP fraud prevention and compensation (p. 1), noting that data may be confidential or market sensitive, the Committee would be grateful if you could:**

    1. **Share information you may have on the financial cost to firms of preventing APP fraud, if possible.**

    2. **Provide an overview of different participants in the banking and payment sectors are impacted by APP fraud, broken down by firm type, e.g., major retail bank, specialist bank, fintech, etc.**

As the largest senders of payments, the largest banks are now able to split any losses with a receiving entity, even if their customers are the most widely scammed and targeted and even if their fraud controls are poor. This will impact a receiving PSP *regardless* of what fraud prevention techniques they have in place.

The UK's 50:50 liability split benefits big banks more than small PSPs - Need a different model (e.g. Singapore on previous page)



Source: PSR

sardine

The nature of being a current account means that the larger banks receive the salary or pension payment and hence these

current accounts have a lot more data about payment flows in/out e.g. where does this individual typically send their money after receiving their salary/pension.

The non-bank PSPs and Fintech apps are typically secondary accounts and hence don't see as much of a consumer's payment activity. Consequently, they are more likely to see a new payee and due to lack of enough data, they are more likely to see more false positives i.e. more likely to block outgoing payments because they don't have much information about the payee.

Net winners tend to be major retail banks
Net losers tend to be PSPs and Fintech companies (or specialist banks)
We lack data outside the PSRs published data

Sardine has proposed:

- An anonymous benchmarking capability for this data
- Data sharing between large banks and smaller firms, and non banks.

*We strongly recommend***:** The UK puts to tender for private sector firms to bid for both the data sharing and the benchmarking capabilities. The UK considers its faster payments scheme national infrastructure. Such a data sharing and fraud prevention utility should also be national infrastructure.

2. **In response to Lord Vaux's question on what the Information Commissioner's Office (ICO) could do to clarify data sharing rules to facilitate improved fraud detection (p. 4), Mr Taylor noted that was not able to provide specific examples at that time. In response to this, please answer the following:**

    1. **Please provide examples of what regulators and Government agencies, including the ICO, do to improve data sharing between firms and law enforcement, and financial services firms and technology companies.**

I recommend the ICO take specific action to clarify cross-departmental data sharing by establishing a Joint Financial Crime Data Framework in partnership with the Home Office, FCA, and National Crime Agency.

This framework should:

- Establish precise protocols for real-time data sharing between the
  NCA's Financial Intelligence Unit and retail banks when Suspicious Activity Reports indicate mule account networks. Currently, this information often moves too slowly between agencies.
- Create clear rules for when Payment Service Providers can share device fingerprinting data with the National Fraud Database, addressing the current uncertainty that leads many firms to withhold potentially valuable fraud indicators.
- Define exactly how the ICO's requirements align with the FCA's Financial Crime Guide, particularly around transaction monitoring data sharing. This would resolve the current situation where firms receive seemingly conflicting guidance from different regulators.
- Set specific timelines for data sharing responses: 24 hours for urgent fraud cases, 72 hours for standard cases, bringing consistency to current ad-hoc arrangements between agencies.

The ICO should also clarify how their requirements interact with:

- The Economic Crime Bill's data sharing provisions
- The Payment Systems Regulator's Faster Payments fraud requirements
- The National Economic Crime Centre's information sharing frameworks

I recommend the ICO consult on technical specifications that clearly state when and how financial institutions can share specific data points like device identifiers, transaction patterns,

and known fraudulent indicators.

Sardine has formed multiple working groups to provide expert guidance on this subject.

To illustrate this practically: When a bank identifies a mule account, current guidance doesn't clearly state whether they can share the associated device fingerprints with other banks in real-time. The ICO should explicitly confirm that sharing such technical identifiers, when there is clear evidence of fraud, falls within the public interest processing ground under UK GDPR Article 6(1)(e).

3. **In response to Lord Lilley's question as to what changes would improve the operation of the regulator, in addition to the clear, specific examples provided by Mr Taylor and Mr Ranjan, (p. 6) Mr Taylor offered to discuss in more detail ways to improve the UK's competitiveness and the metrics that would measure this (p. 7). In response to this, please answer the following:**

    1. **Please suggest three key regulatory changes that would improve the competitiveness of the UK in your sector.**

    a) *Create a Global Digital Identity Passporting System* – Similar to Estonian e-residency. The UK should establish a sovereign digital identity framework that combines strong KYC standards with international interoperability. This would build on the success of open banking but go further by:

    * Creating a standardized API that allows UK-verified identities to be recognized by financial institutions globally
    * Establishing mutual recognition agreements with the EU, Singapore, and UAE financial centers
    * Setting clear liability frameworks for identity verification across borders

* Reducing onboarding costs for fintechs by an estimated 60-70%

b) *Implement automated reporting through standardized APIs, cutting compliance costs by an estimated 40%*

The banking sector has pushed back on this when it was first discussed in the mid 2010s, but it would dramatically reduce the cost of creating and successfully running a regulated Fintech company, it would also improve the data quality in oversight at the regulators. This would require significant upskilling.

c) *Create specific zones where UK-regulated entities can passport their services with minimal additional oversight* (similar to how EU firms passport banking licences and MTLs), starting with

* Singapore
* UAE
* Aligning digital asset regulation with the USA post MiCA

The goal is for these to be binding mutual recognitions rather than loose cooperation. This would be ambitious world first and difficult to achieve but would make the UK wildly competitive. It would unlock cross-border payments, and make the UK the obvious destination for an HQ between Asia, the MENA and the Americas.

2. **Please suggest metrics that could be taken forward by the regulators that would allow internal leadership and Parliament to better understand their progress on reducing fraud and increasing the UK's competitiveness.**

   Fraud Detection Speed – Time between first interaction/transaction and regulatory or law enforcement intervention. Compare this to global peers in partnership through the G7 or G20 (getting this data could be a challenge for global benchmarking, but simply measuring it could be instructive).

Intervention impact score – Recovery rate of funds from regulatory interventions (again, getting this data would be hard)

Data shared by institution type – Are banks, fintech companies and PSPs sharing data? If so how often compared to their peers?

Sector specific APP Fraud rates per sending and receiving entity (e.g. PSPs are very different to banks, banks have more data). It becomes Apples to Oranges without this context.

10 January 2025