SWIFT Response

HM Treasury

Call for Evidence on Data Sharing and Open Data in Banking

25 February 2015

Foreword

SWIFT thanks HM Treasury for the opportunity to respond to the Call for Evidence on Data Sharing and Open Data in Banking.

SWIFT is a member-owned, cooperative society headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholding users, comprising more than 3,000 financial institutions. We connect more than 10,800 connected firms, across more than 200 territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides market infrastructures, banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

We thank HM Treasury again for the opportunity to comment. Please do not hesitate to contact us should you wish to discuss any of the contents set out herein any further.

Natasha de Terán

SWIFT | Head of Corporate Affairs
Tel: + 44 20 7762 2151
Mob: + 44 7780 483 467
www.swift.com

Contents

1 General Comments 4

2 Responses on the Call for Evidence Questions 5

2.1 Question 1. What benefits and risks could arise from an open API standard? 5

2.2 Question 2. What can the government do to facilitate the development and adoption of an open API standard? 5

2.3 Question 3. Who should play a role in the development of an open API standard and who should be able to make use of it and how? 5

2.4 Question 4. What are the costs likely to be for banks, or other financial services firms and providers of credit, developing an open API standard in banking? 6

2.5 Question 5. The government would like to deliver an open API standard in banking as quickly as possible. Are there practical issues which could affect quick delivery? Would 1 to 2 years be a reasonable timescale for delivery? 6

2.6 Question 6. What issues would need to be considered in terms of data protection and security, and what is the best way to address these? 6

2.7 Question 7. What are the technical requirements that an open API standard should meet? 7

2.8 Question 8. What benefits do respondents see from the publication of more open data in banking? 7

2.9 Question 9. What issues would need to be considered in terms of data protection and security, and what is the best way to address these? 7

2.10 Question 10. What are the other risks or costs of publishing more open data in banking, and how can they be addressed? 7

1 General Comments

The main focus of our response is on the need for engagement with the appropriate industry standard-setting bodies in the development of an open API to enable data sharing in banking. Such bodies provide a useful template for the good governance which will be essential if the aims of the open API are to be realised.

SWIFT is a key contributor to the development of secure open standard industry solutions and tools for the exchange of data related to financial transactions and our response draws on this experience. We would be pleased to contribute our expertise to the forthcoming discussions on moving this important initiative forward.

2 Responses on the Call for Evidence Questions

Q1 What benefits and risks could arise from an open API standard?

Please see our response to Q6, below.

Q2 What can the government do to facilitate the development and adoption of an open API standard?

Her Majesty's Government should ensure that it engages with the industry, and in particular with the appropriate open standards-setting bodies that we have highlighted in our answer to question Q3 below. The Government should pay particular attention to the governance arrangements for the open API, and in this regard we think it right that such industry standards should follow the principles of good governance used by international bodies such as ISO (International Organisation for Standardisation), which we also cover in more detail in our answer to Q3 below.

It is also important that the development of the open API is consistent with other initiatives which will cover the same or similar concerns. Of particular relevance are the communications standards which will be required to enable new payment service providers (PSPs) to access account information from Account Servicing PSPs (Banks) under the EU Payment Services Directive revisions (PSD II). Under PSD II, the European Banking Authority (EBA) will be responsible for the development of regulatory technical standards with which all PSPs will have to comply to enable secure communications between Account Servicing PSPs and third party service providers. Government and regulators must ensure a coordinated approach so that industry can have confidence that developments made for one purpose will not need to be revisited in short order for another.

Q3 Who should play a role in the development of an open API standard and who should be able to make use of it and how?

The financial industry already depends on a number of important standards processes to enable efficiency in its communication infrastructure and to reduce associated costs. This is true for all financial communications, whatever the business domain or the communication network, and it applies whether the counterparties are financial institutions, clients, suppliers, market infrastructures or public authorities.

Many of the standards upon which the financial industry relies are governed by the International Organization for Standardization (ISO). ISO was formed in 1947, with a mission 'to facilitate the international coordination and unification of industrial standards'. Today ISO is a network of 163 national standards bodies, each of which represents ISO in its country. ISO manages 19,500 international standards in a wide variety of industries. The ISO organisation is based in Geneva and employs around 150 staff, but the wider organisation consists of 100,000 volunteers drawn from national standards bodies and industry 'liaison organisations', such as SWIFT. Industry specialisation is at the level of Technical Committees (TCs).

Standards are developed by expert users in the relevant industry; ISO oversees and facilitates the process, and publishes the results in the form of new or revised standards. New or revised standards are approved by ballot. Votes are cast by the national standards bodies represented on the relevant ISO TC. In the UK, the national standards body is the British Standard Institute (BSI), and the committee responsible for national Financial Services standardisation is BSI IST/12 Financial Services, operated under contract to BSI by the Payments Council.

One example of such a standard is ISO 20022 - the Universal Financial Industry Message Scheme. ISO 20022 defines the platform for the development of financial message standards. Its business modelling approach allows users and developers to represent financial business processes and underlying transactions in a formal but syntax-independent notation. These business transaction models are the "real" business standards. They can be converted into physical messages in the desired syntax for example XML (eXtensible Mark-up Language) or ASN.1.

In SWIFT's view, it is essential that an "open" standards-based approach is adopted for the development of the open API standard. Furthermore, we believe that the various bodies, including SWIFT, that contribute to the relevant standards development process outlined above should be key contributors to the process for the development of the open API.

Q4 What are the costs likely to be for banks, or other financial services firms and providers of credit, developing an open API standard in banking?

Applying a well-known and proven process, such as the one outlined in Q3 above, to the development of a new open API standard for banking will have a positive impact on both development and adoption costs. The ISO standards initiatives are generally driven by communities of users looking for more cost-effective communications to support specific financial business processes with the aim of facilitating interoperability with existing protocols.

The ISO 20022 standard mentioned in Q3 is a global standard covering all financial domains. It is also based on a common 'business model' - a formal structure similar to a conventional dictionary (i.e. a repository of terms with their definitions), but with the added ability to capture the relationships between terms. It also ensures a very high level of semantic interoperability based on the precise definition of data elements exchanged, irrespective of the message syntax. This offers a way of shielding investments from future syntax changes by proposing a common business modelling methodology to capture, analyse and describe processes and their information requirements. The ISO 20022 business model is described further under Q10, below.

Additionally, as ISO 20022 is increasingly used by payments systems and other financial market infrastructures, an approach based on ISO 20022 could provide re-use benefits for banks that already use the standard to connect to those infrastructures.

Q5 The government would like to deliver an open API standard in banking as quickly as possible. Are there practical issues which could affect quick delivery? Would 1 to 2 years be a reasonable timescale for delivery?

In order to meet a timescale of 1 to 2 years for delivery of a new open API standard, SWIFT recommends applying existing methodologies, data models and definitions such as those specified by ISO 20022. The ISO 20022 standard can be used to define and formalise the data exchanged in the open API.

If the API is to be delivered in a short timescale, SWIFT recommends that wherever possible existing internationally recognised identification schemes for business parties and other key reference data elements are specified, including those defined by the following ISO standards:

ISO 9362 – Business Identifier Code (BIC)
ISO 13616 – International Bank Account Number (IBAN)
ISO 17442 – Legal Entity Identifier (LEI)

Q6 What issues would need to be considered in terms of data protection and security, and what is the best way to address these?

An open API that provides access to private account and transaction data across banks would be a high-profile target for attackers, even more so if the API provides the possibility of initiating payment transactions. The proposed use of the OAuth 2.0 framework with only usernames and passwords to authenticate users provides insufficient guarantees to prevent security breaches.

OAuth 2.0 is presented as 'simple', and while that is mostly true for the API consumer (the "Data App"), it is not so true for the API service provider (the "Bank"), which needs to have sound expertise and make careful implementation choices in order to prevent breaches. OAuth 2.0 by itself is not a standard protocol that guarantees interoperability, and it provides many choices and options, not all of which are relevant to an open banking API. Moreover OAuth 2.0 is extensible with different techniques such as SAML 2.0 Bearer tokens, MACs, and Open ID Connect. This could present consumers of the API with a wide variety of somewhat different APIs.

To overcome these challenges, the industry should combine its expertise, and agree on how OAuth 2.0 should be used for authorising access to the open banking API, and how authentication of users and of client applications would be handled. A standardisation body such as ISO, or a neutral bank-owned cooperative such as SWIFT, could help facilitate this. A peer-reviewed process is the best guarantee of high quality.

Alternatively, or additionally, banks could appoint an 'API facade' provider, which would act as a front-end towards the consumers of the open banking API. The API facade provider could shield the banks from many attacks. This could also relieve banks from much of the burden of implementing this API securely,

by allowing them to re-use some of the established secure channels that exist today between banks and facade providers. The API facade would also guarantee uniformity of the API towards the API consumers. This could speed up the implementation of the open banking API, and reduce the costs of implementing the API across the industry.

Applications could, over time, collect authorisations to access thousands, if not millions of accounts. A security breach in such an application could lead to personal account data being made public on the internet, and such a breach would destroy the public trust in the scheme. Users and SMEs will have to trust the applications and third parties that want access to their account data or transaction history, and to that end, strict and legally binding rules should be established regarding the protection that applications and third parties must provide for data after it has been accessed over the API.

For this reason, a method of certifying applications and third parties must be established, and ongoing audits and checks should be carried out for certification status to be retained. Furthermore, the user or SME must have the means of checking if the application or third party is certified, for example, by consulting a public registry. The user or SME must also be able to limit the access of the application or third party in scope or time, for example by limiting access to 'only account balances, but no transaction history, and only for the last six months'. In addition, there should be assurances that the application will not store the data long-term without explicit permission, and it should be possible to check which personal data was previously obtained and stored by the application, and to request the deletion of all or part of this personal data. Finally, the user or SME should be able to revoke access granted to an application or third party.

Q7 What are the technical requirements that an open API standard should meet?

Please refer to our answer to Q6.

Q8 What benefits do respondents see from the publication of more open data in banking?

Q9 What issues would need to be considered in terms of data protection and security, and what is the best way to address these?

Please refer to our answer to Q6.

Q10 What are the other risks or costs of publishing more open data in banking, and how can they be addressed?

If the purpose of open Banking APIs is to be fully achieved, it is important that all banks interpret the specification of data exchanged in the APIs consistently. Without this consistency, data from different banks cannot be meaningfully compared or aggregated. This challenge is familiar from the world of financial messaging standards, and the industry has evolved organisational structures and methodologies to discuss, define, agree and publish precise shared definitions for key concepts.

As noted above, ISO 20022 is the ISO approved standardisation methodology for financial messages and data sets. It includes precise definitions for key financial industry concepts. These definitions are maintained in a 'business model' that has the added ability to capture the relationships between terms. For example, the ISO 20022 Business Model defines the term 'account', but also captures that there are different types of account (cash, securities, etc.) that nevertheless share some common attributes; that an account has an account owner, and an account servicer, that the account servicer is a financial institution, and so on. The business model also defines the format or data type of individual data items, be they dates, amounts, text, codes or larger structures such as name and address.

The content of the business model is defined and maintained by the users of the standard, subject to a strong registration and governance process that ensures consistency and quality. We believe that the precision of the definitions found in ISO 20022, combined with the open but rigorous process for adding new content, makes it an excellent resource for ensuring that data elements specified in the context of banking APIs are interpreted consistently by implementers.

**** END OF DOCUMENT ****