**Business Justification**

**for the development of new ISO 20022 API resources as ISO 20022 financial repository items)**

*Note: the purpose of this document is to give guidelines to organisations that want to develop new candidate ISO 20022 API resource definitions. Such requests are subject to the approval of a business justification by the ISO 20022 Registration Management Group (RMG). Please consult the iso20022.org website for additional details on* [*the registration process*](http://www.iso20022.org/development.page)*. The business justification must include the following captions, as described.*

1. **Name of the request:**

Anomaly Markers API resources

1. **Submitting organisation(s):**

Swift

1. **Scope of the new development:**

The proposed API resources will support the exchange with Financial Institutions (FIs) of insights (the anomaly markers) that could be symptomatic of financial crime (for example, fraud) and/or of operational issues (for example, duplicate payments, clerical mistakes). These insights are meant to support FIs in detecting payment anomalies and act on them.

The ISO 20022 business area is currently the one of Payments services but could be expanded to other areas such as Trade going forward.

Five resources (aka anomaly markers) categories have been identified:

* New Account Scenario: allowing to detect new or dormant account numbers as well as new or dormant currencies for a given account number(s);
* Repetitive Payments: allowing to detect payments sharing similar or equal amount and currency exchanged by/from/between account number(s);
* Activity Spike (aggregated amount): allowing to detect increases of aggregated amounts exchanged by account numbers;
* Activity Spike (exchanged messages): allowing to detect increases of the number of exchanged messages by account numbers;
* Problematic account reuse: allowing to flag account numbers reported in previous anomaly signals (returned or rejected payments, recalled payments).

The resources leverage the following information, both as input as well as to compute the data provided as output:

* Debtor Agent
* Debtor Account (fields allowing the identification of the account number, excluding therefore other Personal Identifiable Information)
* Creditor Agent
* Creditor Account (fields allowing the identification of the account number, excluding therefore other Personal Identifiable Information)
* Interbank Settlement Amount

The resources and information are based on the current understanding and may both evolve in discussions with the Swift Anomaly Detection Working Group.

Here is the technical flow illustrating the different steps:



The diagram highlights that the consuming FIs will have the possibility to consume one, several or all resources at once. As the resources are tied to an account number or a pair of account numbers, the consumption of more than one resource simultaneously implies that in such a case, the response will be associated to the provided account number or pair of account numbers specified in the request.

The triggering event for a FI to request one or more resources is the need for the FI to verify whether a payment is exempt of anomalies that would require further investigation before being instructed.

Upon the identification of such a need, the FI will have the possibility to request one or more resources and those will be returned by the Data Provider. The Data Provider could be:

* another FI
* a Software Vendor having access to that information
* a Payment Network provider.

Given the sensitive nature of the data leveraged to compile the anomaly markers, any Data Provider of those, will have to ensure that they do comply with local legislation.

Upon reception of the response, the FI will be sole responsible of acting on it.

The resources are being created with input from members of the Swift Anomaly Detection Working Group which comprises of global banks. While the resources are being created, we welcome requests from the review committee to fill any remaining content gaps to make it truly global in usability.

1. **Purpose of the new development:**

Payment anomalies, many of which are caused by fraud, are a challenge for the financial industry. Indeed, once a payment is settled, it can be difficult or impossible to recover funds. So as payments settle faster it becomes increasingly important to identify abnormal transactions promptly and accurately. Growing volumes of reported fraud also put additional pressure on FIs to detect and act on payment anomalies to ensure a safe and end-to-end frictionless payment experience.

It is well understood that financial crime, such as fraud, cannot be solved by Fis individually and that global collaboration is required to reinforce the industry’s defenses. Authorities worldwide are encouraging collective action between Fis, law enforcement agencies and other stakeholders to share information on emerging fraud trends and to implement collective measures, such as anomaly detection in payments, to combat fraud effectively.

The new ISO 20022 resources scoped by this document allow defining new standards associated to the sharing of such information, supporting fIs with the detection of payment anomalies. There is no standard existing today, however, as the industry is keen in addressing the payment anomaly challenge, it would also benefit from a common standard that could be used across various payment rails.

1. **Community of users and benefits:**

In its IC3 report, the FBI reported that the fraud losses in USD denominated payments accounted for $10.3bn in 2022. In its 2022 Banking Operational Risk loss data report, ORX wrote that the losses associated to operational issues between 2016 and 2021 accounted for $600bn.

These statistics do not have the ambition to be exhaustive but rather to highlight that payment anomalies are a problem for the financial industry and is likely to remain one as long as the industry does not try to address it as one.

While the resources have been developed by Swift, they reflect the needs of fIs part of the Swift Anomaly Detection Working Group which are transversal to the payment rails fIs use.

By registering these ISO 20022 resources, Swift aims at making the community requirements gathered through its working group, available to the entire industry for it to kick start the development of similar capabilities. Indeed, the fight against fraudulent activity and the detection of other forms of payment anomalies is an activity that should be undertaken as one; given the negative impacts that these problematic payments have on fIs, on the G20 goals for cross border payments but also, and foremost, on end-customers. The open ISO 20022 resource will also enable global scaling for solutions

The emergence of regulations around similar capabilities such as Confirmation of Payee (aka IBAN-name check) highlight the importance and timeliness of such anomaly markers.

1. **Timing and development:**

Swift aims at starting the implementation of the described resources (aka anomaly markers) in the course of 2024. Making these resources public will allow other organizations to comment the proposal, make any adjustments to it both in terms of generalization of the specifications as well as of refinement to cater for additional payment anomaly detection requirements.

As described in previous sections, the resources represent the outcome of discussions held by Swift via its Anomaly Detection Working Group, a group constituted by 12 fIs having an international presence.

1. **Commitments of the submitting organisation:**

Swift confirms that it can and will:

* undertake the development of the candidate ISO 20022 API resource models that it will submit to the RA for compliance review and evaluation. The submission must be compliant with the [ISO 20022 Master Rules](http://www.iso20022.org/documents/general/ISO20022_MasterRules.ZIP) and include a draft Part 1 of the ISO 20022 Resource Definition Report (RDR) compliant with the [template for RDR part 1](http://www.iso20022.org/documents/general/ISO20022_MasterRules.ZIP) provided by the RA and, optionally, examples of valid and invalid instances of each candidate ISO 20022 API resource.
* address any queries related to the description of the models and ISO 20022 API resources as published by the RA on the ISO 20022 website.

Swift confirms that it will promptly inform the RA about any changes or more accurate information about the number of candidate ISO 20022 API resources and the timing of their submission to the RA. If the submitting organisation does not submit the candidate ISO 20022 API resources within the timing announced in section F and does not inform the RA beforehand, the business justification may lapse and require re-submission of a new business justification for approval by the RMG.

Swift confirms its intends to organize a business review of the candidate ISO 20022 API resources ahead of the review and qualification by the RA and before their submission to the SEG(s), API SEG, BMST and/or TSG for approval. Thanks to this review, Swift does not anticipate additional testing activities such as piloting. The completion of the business review should happen end of H1 2024.

Swift confirms it is committed to undertake the future maintenance of the ISO 20022 API resources scoped in this request.

Swift confirms its knowledge and acceptance of the ISO 20022 Intellectual Property Rights policy for contributing organisations, as follows.

*“Organizations that contribute information to be incorporated into the ISO 20022 Repository shall keep any Intellectual Property Rights (IPR) they have on this information. A contributing organization warrants that it has sufficient rights on the contributed information to have it published in the ISO 20022 Repository through the ISO 20022 Registration Authority in accordance with the rules set in ISO 20022. To ascertain a widespread, public and uniform use of the ISO 20022 Repository information, the contributing organization grants third parties a non-exclusive, royalty-free licence to use the published information”.*

1. **Contact persons:**

Jean-Francois Grange, Jean-Francois.GRANGE@swift.com, +32473663303

Tom Alaerts, Tom.ALAERTS@swift.com, +852 6656 8576

Serge Ioanidis, Serge.IOANIDIS@swift.com, +32491622771

1. **Comments from the RMG members and relevant SEG(s) or SubSEG(s) and disposition of comments by the submitting organisation:**

This section will include the comments received from RMG members and the SEG(s), SubSEG(s), API SEG, BMST and/or TSG, if any, and the response given to each of these comments by the submitting organisation.

**Comments from the Canadian delegation**:

We could not find any corresponding ISO 20022 message in the current portfolio, and the Business Justification (BJ) only refers to leveraging existing resources, not existing ISO 20022 messages.

There might be an opportunity to create a new set of ISO 20022 messages for the purpose of detecting payment anomalies as described in this BJ. That would not only allow the standard to be applied globally to a more broader range of payment systems (e.g. those which are not API enabled) but may also be used as a payload in the API resources proposed in this BJ or any similar requirement in the future. With the current approach, it seems like the standard will be limited to the data providers which can use APIs for communication with the fIs.

**Reply from submitting organisation:**

We believe that the resources required to support the so-called Anomaly Markers, reviewed by the Swift Anomaly Detection Working Group, are generic enough to be reused indistinctively via API or messages.

That being said, the creation of new dedicated ISO 20022 messages and/or update of existing ones, to convey the Anomaly Markers resources, has not been considered at this stage but could of course be at a later stage, depending on the business needs.

This would however require an additional Business Justification, one dedicated for the creation and update of corresponding new or existing ISO 20022 messages.

**Comments from the Finnish delegation:**

OP recommends specifying the data provider role in more detail. In target state Data provider role should be only available for those parties that are sufficiently regulated and supervised to ensure:

* Quality and the trustworthiness of the data behind the anomaly markers.
* That input data is managed accordingly to those regulations and laws as required from the FI that inputs the data. One example of this type of regulation would be GDPR in EU.

**Reply from the submitting organisation:**

We believe that the consumers of such Anomaly Markers should ensure that these comply with their local regulation(s) (eg. DORA, GDPR). The API resources define the elements to be exchanged and they only provide a way to carry the information in an open-source approach.

A note has been added to invite any Data Provider to perform such a due diligence, but this would not substitute the consuming parties to ensure that these activities have been well performed and match with their own requirements or regulatory obligations.

**Comments from the Swiss delegation:**

The Swiss Association for SWIFT and Financial Standards (SASFS) is the representative organisation for financial standardisation in the financial centre of Switzerland and Liechtenstein.

The Swiss standards experts of the SASFS have reviewed the BJ and support its underlying intent. The following are a number of suggestions for how to move forward the BJ and the proposed API resources.

In view of the development and employment of the proposed API resources, we would like to make the following suggestions:

• High amounts regardless of previous activity to mitigate substantial money outflow

• Use user session data (IP address, Browser, Smartphone Details,…) to detect device switches

• Generally make sure to allow for many auxiliary attributes that turn out to be effective to identify fraud cases (birthday or age of the sender, age of the 2 factor authentication device,…)

• behaviour detection data: typing, mouse movement pattern, voice or camera input metrics, fingerprint input,…

• Use known high focus account numbers based on reported fraud receiver addresses

In view of the potential future application of the proposed API resources in the trade finance space, we would like to make the following comments:

As we understand it, payments are checked for anomalies when they are made.

A letter of credit/guarantee is an obligation to make payment at a future date if certain conditions are met.

A check at the time of payment would therefore be“"too lat”" and might even prevent us from fulfilling our obligation.

In the trade finance space, we therefore check a transaction at the time of issue, not at the time of payment.

We always make payments from letters of credit/documentary collections/guarantees either to a customer or to a correspondent bank, whereby the originator of the outgoing payment is always the paying bank. The Anomaly Markers API resource will not (be able to) provide much added value for a payment bank to its customer or bank in favour of a correspondent bank.

The obligation under a letter of credit/guarantee is a conditional payment to a legal entity, not to an account. At the time of utilisation, the beneficiary indicates the account to which the payment is to be made. In most cases, the beneficiary is a customer of the bank and the“"paymen”" is made accordingly as a simple account credit.

As the Anomaly Markers API resource is heavily based on account details, however parties are relevant in trade finance, the resource will be of little use in the form foreseen. On the other hand, trade finance transactions are already intensively scrutinised for compliance (AML, terrorist finance, diversion point countries, etc.) and sanctions topics, which include questions of customary practice, compatibility with the purpose of the company, volume in relation to the availability of goods, etc.

**Reply from the submitting organisation:**

Thank you for all these detailed suggestions of improvements. Please find here below our answers, for each of those:

* *High amounts regardless of previous activity to mitigate substantial money outflow.*

This Anomaly Marker has been considered together with our community and more specifically the Swift Anomaly Detection Working Group. However, we see a risk in it as it could provide commercially sensitive information and be abused by Requestors. A partial trade-off could consist in producing generic alerts as soon as the amount would exceed a certain threshold, established for instance on the basis of the average amount exchanged by an account. Such an approach would nevertheless generate quite some noise (false positives).

* *Use user session data (IP address, Browser, Smartphone Details,…) to detect device switches.*

While it is clear that telemetric information is a great asset in detecting certain forms of fraud, this information is not conveyed in Payments messages which are the source of information that will be used to determine the Anomaly Markers. We see the addition of such additional data points addressed in a separate Business Justification.

* *Generally make sure to allow for many auxiliary attributes that turn out to be effective to identify fraud cases (birthday or age of the sender, age of the 2 factor authentication device,…)*

While it is clear that these auxiliary attributes are a great asset in detecting certain forms of fraud, this information is not conveyed in Payments messages. To make the proposed resources as generic as possible, some of these attributes will be foreseen in the resources, even though their delivery may not always be achievable depending on the nature and data access of the Data Provider.

* *behaviour detection data: typing, mouse movement pattern, voice or camera input metrics, fingerprint input,…*

While it is clear that biometric information is a great asset in detecting certain forms of fraud, this information is not conveyed in Payments messages which are the source of information that will be used to compile the Anomaly Markers. We see the addition of such additional data points addressed in a separate Business Justification.

* *Use known high focus account numbers based on reported fraud receiver addresses*

This Anomaly Marker is indirectly foreseen in the proposal and will be obtained by combining the CreditorAccount information (address) to the Problematic Account Reuse marker (account number reported as problematic).

With regards to the additional comments related to Trade, we take note of these and propose, for time-to-market reason, to focus solely in a first iteration on Payment messages and the information that those convey and that can be used to compile the Anomaly Markers presented in this Business Justification.

**Comments from the Norwegian delegation:**

We are all positive to the initiative.