Transaction Data Usage
Swift Information Report, IR 927

Confidentiality Level 2
Distribution to National Member Group allowed

Purpose of the paper
This paper aims to inform the community about a potential evolution of the current Transaction Data and Governance Usage Framework (TDGUF), introduced in December 2018 (ER1887). Building on the strong governance foundation and robust controls already in place, it outlines a proposal to strengthen and expand the conditions under which Swift may analyse and leverage transaction data, with the goal of delivering greater strategic value and benefits to the community.

Triggers for the paper
The rapid pace of innovation in the global financial sector is reshaping both competition and collaboration, creating valuable opportunities for Swift to responsibly leverage transaction data to support the community in navigating emerging opportunities. Strategic use cases have highlighted the value of doing so and informed a proposed update to the existing framework and safeguards, aimed at providing greater clarity and enabling innovation within well-defined boundaries.

Action required
This paper is for information.

Governance
Risk Committee and Board

Issued by
Thomas Delaet, Nathan Van de Velde

1 Summary

Innovation and change across the global financial industry have accelerated, with emerging technologies and evolving customer expectations reshaping competition and collaboration across both payments and securities. In this context, Swift has identified opportunities to unlock greater value from transaction data to enhance customer experience, deliver richer insights, and execute key strategic initiatives (e.g. new payments scheme). To realize this potential for the benefit of the community, Swift is proposing an evolution of the Transaction Data Governance and Usage Framework (TDGUF), including clearer safeguards and guidance. This update reflects the industry's trajectory and ensures alignment with Swift's governance principles.

This paper proposes an evolution of the TDGUF to enable Swift to deliver more value to its customers, while maintaining strong oversight of transaction data use. The framework would shift from a product-centric to a purpose-driven model, allowing upfront agreed purposes to support multiple use cases and thereby improving agility and time-to-market. It also introduces the ability to deliver more granular insights for community-benefiting offerings. Strategic oversight would remain with the Board, while day-to-day governance continues under the existing, proven framework—further reinforced with enhanced controls.

Crucially, this is an evolution and not a reinvention of the existing framework, adapted to align with the new Swift governance model while preserving (and arguably strengthening) the trust and safeguards already in place.

2 Context and opportunities

In December 2018, Swift adopted a TDGUF (ER1187) to strengthen the governance of transaction data. The framework was designed to evolve from the Board's detailed, case-by-case approval for using transaction data at each individual message field-level toward a principles-based approach that enabled Swift to operate with greater agility, while maintaining robust safeguards to ensure data security, privacy, and regulatory compliance.

The framework is defined by **ten principles**. These principles cover proportionality and intended audience, Board approval and transparency, security and confidentiality, and data granularity. The ten principles are detailed in Attachment 1.

ER1187 also established the **Secure Data Lab** (SDL), a highly secure environment where Swift may have access to full transaction data for statistical analysis for its own product development and technical optimization purposes. The results of such statistical analysis are anonymised and where possible aggregated and thus do not reveal the identity of SWIFT customers, individuals, other third parties, or their business relationships. The SDL has been instrumental for the safe development and assessment of products and services using live data prior to launch. It has also driven innovation.

Management accountability was reinforced through the creation of the Swift **Transaction Data Steering Committee** (TDSC). The TDSC replaced the annual Board approval cycle with more regular, six-weekly reviews and approvals of new requests for the use of transaction data covering internal use, enrichment of existing commercial offerings, and exploratory work in the Secure Data Lab (SDL).

After seven years, the TDGUF has provided a strong governance foundation, and proved its effectiveness. The TDSC, which comprises the Chief Product Officer, Chief Operating Officer, Chief Technology Officer, General Counsel, Data Protection Officer, together with senior experts from Risk, Security, and Privacy has in fact significantly increased the level of scrutiny applied to the use of transaction data, both in assessing business justifications and in reviewing technical implementations.

But more can be done. In today's rapidly evolving environment, transaction data offers unique insights into market dynamics, emerging instruments, customer behaviour, and risks — insights that are critical for shaping strategy and ensuring the successful launch of future services. The examples below illustrate use cases that remain constrained under the existing governance model. governance.

Use case 1: Support the ISO 20022 migration. Swift's contingency solution and in flow translation service supports institutions not ready for ISO 20022 after November 2025. Analysis done in the SDL indicated that some institutions may face transaction rejections. However, under current TDGUF, specifically principle 9 which requires anonymization at the Swift customer level, the analysis output prevent Swift from identifying the institution outside the SDL. This restriction prevents Swift from engaging directly with those institutions to provide targeted feedback and support, limiting the ability to proactively mitigate risk and ensure a smooth migration.

Use case 2: Strategic intelligence for a new retail cross-border payments scheme. Swift is exploring a new retail payments scheme to address evolving market needs and customer expectations. Monitoring its success requires granular insights, such as measuring speed improvements and detecting hidden fees. Current SDL principles (anonymisation at Swift customer level) prevent sharing these insights directly with customers for feedback (Principle 9 of the TDGUF framework – see Attachment 1). This limitation reduces the ability to validate performance and optimize the scheme in collaboration with the community.

Use case 3: Reuse data and analytics across products. Payment segmentation (e.g., retail vs wholesale) derived from message data identifying the parties involved, is a key piece of metadata for understanding market behaviours and identifying opportunities. For example, it supports the automatic identification of payment categories and the automated processing of transactions based on those categories. Under the current TDGUF, each new use of this data requires explicit Board approval (Principles 3 and 4), which introduces delays and limits the ability to leverage insights across multiple contexts. Evolving the framework to allow purpose-based approvals would enable Swift to reuse data responsibly to generate insights that inform strategy and community needs, while maintaining strong governance.

2.1 Proposed changes

The current TDGUF sets out ten principles that define the criteria, boundaries, and controls for transaction data use. We propose evolving three of the ten principles (Principles 3, 4 and 9 to address the limitations illustrated by use cases 1, 2 and 3 above) while preserving existing safeguards by leaving the other seven unchanged. This would allow to streamlined approvals, enable wider reuse of data across products and channels, and deliver more granular insights, while preserving the robust safeguards (including compliance with applicable personal data protection laws) that have proved effective over the years.

Concretely, we propose the following changes:

- **Adopt a purpose-driven approach**. Shift from the current product-centric, single-use Board approvals to a purpose-driven approach, enabling multiple data usage across varied known and emerging use cases within the purposes agreed by the Board. This will enhance responsiveness and accelerate time to market.

- **Reinforce Board strategic oversight**. The Board will approve a defined set of purposes for transaction data usage, reinforcing strategic control and alignment with community interests.

- **Streamline operational governance**. **Day to day governance** of the use of transaction data within approved purposes will be managed by the well-established TDSC, ensuring continuity, efficiency and compliance with governance with regular reporting to the Board.

- **Enable more granular data exports from the Secure Data Lab. Allow controlled exports of granular data** at Swift customer (BIC) or financial instrument (ISIN) level from the SDL to facilitate new offerings that support the community.

In parallel, all existing controls are maintained, with additional measures introduced to further strengthen oversight and governance.

- The seven unchanged principles ensure that all existing safeguards, including personal data protection law compliance, confidentiality, security, access controls, and data retention, remain fully preserved.

- There is no change to the existing security framework.

- **New:** Oversight of the TDSC is further reinforced through periodic internal audits of its processes and activities, with reporting to the Board.

In addition, Swift's default internal governance, organizational and technical controls ensures that Swift continues to process transaction data in accordance with the regulatory requirements and our contractual obligations as described in the Personal Data Protection Policy and Data Retrieval Policy.

The changes proposed would impact Principles 3, 4 and 9 as are highlighted in Table 1 below.

Principles	As-is language	Proposed To-be language
Principle 3	The **Board** continues to approve any new commercial offering that involves the use of traffic or message data.	The **Board** approves the list of **business purposes** for which Swift may use transaction data. The **TDSC** approves the **use of transaction data within the Board approved purposes (e.g. for existing and new products, internal use, as inferred metrics, R&D,** SDL requests**)** and supervises internal use of transaction data.
Principle 4	The **Board** explicitly approves any new use of message data identifying ordering or beneficiary parties in commercial offerings.	The **Board** approves the list of **business purposes** for which Swift may use transaction data. The **TDSC** approves the **use of transaction data within the Board approved purposes (e.g. for existing and new products, internal use, as inferred metrics, R&D,** SDL requests**)** and supervises internal use of transaction data.
Principle 9	SWIFT may have access to full traffic and message data as required for point purposes and for statistical analysis for its own product development and technical optimization, in a highly secure and protected environment in SWIFT's EU OPC, on a permanent basis. The ability to test products and services using live production data is crucial to detect the variety of real live scenarios and local market practices (e.g. for the development of ISO 20022 translation rules). The results of such statistical analysis will be aggregated and anonymised and thus will not reveal the identity of SWIFT customers, individuals, other third parties, or their business relationships. SWIFT may use such results to improve its products and services and may share high level statistics regarding the research externally.	SWIFT may have access to full traffic and message data as required for point purposes and for statistical analysis for its own product development and technical optimization, in a highly secure and protected environment in SWIFT's EU OPC, on a permanent basis. The ability to test products and services using live production data is crucial to detect the variety of real live scenarios and local market practices (e.g. for the development of ISO 20022 translation rules). The results of such statistical analysis will be anonymised and where possible aggregated and thus will not reveal the identity of SWIFT customers, individuals, other third parties, or their business relationships. **For initiatives related to the list of purposes approved by the Board, Swift may export from the SDL analysis results at a customer level (e.g. BIC) or financial instrument level (e.g. ISIN) to assess the value for the community and demonstrate the impact at customer level.**

Table 1 – Evolution of principles 3 4 and 9 of the current TDGUF

2.2 The proposed business purposes

Swift proposes defining a clear list of business purposes for the use of transaction data, grouped into four categories:

1. **Core operations** – ensuring the continued reliability and efficiency of Swift's services.

2. **Risk, compliance, and security** – supporting the financial community in the prevention of fraud, financial crime, and operational risk.

3. **Customer insights and strategic intelligence** – enabling the delivery of richer analytics and benchmarking to help participants understand community-level insights and performance.

4. **Innovation and product development** – fostering the design and assessment of new capabilities that respond to evolving market and regulatory needs.

All but two of these purposes align with the current use of transaction data under the existing framework. The addition of two new core operations purposes: **supporting new financial instruments** and **facilitating transaction settlement orchestration**, marks an evolutionary step. These reflect Swift's strategic direction and growing role in enabling more intelligent, frictionless, and interconnected financial ecosystems.

Core Operations

- **Support transaction processing** – Enable secure and reliable pre-validation, sending, receiving, displaying, tracking, categorisation and management of financial messages and files.

- **Operational efficiency** – Maintaining, assessing and improving existing Swift services and products within approved purposes anticipating operational issues and support problem diagnostic.

- **Standards management –** Monitoring and reporting Swift standards adoption trends.

- **Support new financial instruments –** Enable secure and reliable pre-validation, sending, receiving, displaying, tracking, categorisation and management of new types of value transfer mechanisms such as digital and wallet payments.

- **Orchestrate transaction settlement –** Enable secure and reliable settlement between multiple settlement mechanisms.

Risk, Compliance, and Security for community

- **Anomaly detection and prevention** – Identify unusual patterns to detect anomalies, operational issues, supporting resilience and risk management.

- **Financial crime prevention & compliance** – Support AML, sanctions screening, and counter-terrorist financing efforts.

Insights and Strategic Intelligence

- **Transaction reporting and benchmarking** – generate aggregated insights for market intelligence, data quality, community benchmarking and industry intelligence.

- **Strategic intelligence** – generate forward-looking insights that reduce uncertainty, anticipate change, and guide long-term priorities to inform decision-making and help shape the Swift's strategy with clarity and confidence.

Innovation, Development

- **Product evolution** – Enhance existing offerings based on aggregated insights and community feedback.

- **R&D and innovation** – Assess opportunities and risks to identify new solutions that deliver value for the SWIFT community in areas where Swift customers are active.

Swift continues to contractually commit not to process or use any transaction data used in an SDL data analysis for the following purposes:

- Sell the direct output of its transaction data analysis to third parties,

- Use the results of its transaction data analysis to allow SWIFT or any third party to send marketing communications,

- Use any insights derived from its transaction data analyses for advertising purposes,

- Perform analytics on transaction data in view of offering products or services other than to SWIFT customers, or

- Perform analytics on transaction data to the sole benefit of third parties.

2.3 Impact of the proposal on the allocation of responsibilities

Table 2 below maps out updated responsibilities under the proposed evolution of the TDGUF.

Category	Body	Details
Decision	Board	• Transaction Data Governance and Usage framework • List of approved purposes • Financial industry body requests for data insights (e.g. BI partnerships)
	TDSC	• SDL requests • Use of transaction data within approved purposes (e.g. in products, for internal use, as inferred metrics, R&D) • Supervision of internal use of transaction data
Consultation	NMG	• Board decisions related to transaction data governance
	Data Protection Working Group (DPWG)	• Board decisions related to transaction data governance • Community-wide initiatives regarding transaction data including personal data, such as change of GDPR status, changes to the transaction data governance framework, use of community data (e.g. account analytics, anomaly markers, creation of the SDL)
	Working/User Group (+ Privacy experts where relevant)	• Use of transaction data including personal data in product-specific initiatives (involving only transaction data of subscribed customers, e.g. g4C)

3 Next steps

We will continue to refine the proposal in consultation with the Board, the community, and relevant advisory committees, including the Data Protection Working Group. Subject to the outcome of these discussions, we plan to submit an Executive Report for Board approval in March 2026.

Attachment 1 – The current Transaction Data Governance and usage Framework

In December 2018, Swift introduced a new Data Governance and Usage Framework (ER1887 – New Framework for Data Governance and Usage). It established ten principles that define the criteria, boundaries, controls, and review mechanisms governing how Swift may analyse and leverage transaction data. Whether for internal usage or for the development of new products or services, the framework ensures security and privacy, regulatory compliance, and strict access controls for authorized parties only.

The existing framework is structured around ten principles, listed below

Proportionality and intended audience

1. Swift will consistently apply the **principle of proportionality**, ensuring that the access to data and the type of information that is used is strictly limited to what is required for the business or technical need and is in line with the objectives stated above. Furthermore, Swift will apply the principle of Privacy by Default (i.e. by default, Swift should ensure that personal data is processed with the highest privacy protection). Finally, Privacy Impact Assessment will be done when deemed appropriate.
2. Swift transaction data products and services derived from transaction data analysis are available to the **Swift community** only (i.e. Swift users), and Swift will not commercialise any such data to third parties. Sharing transaction data beyond the Swift community is subject to explicit Board approval, under the existing documented business intelligence partnership principles approved by the Board. These are outlined in Attachment 2.

Board approval and transparency

3. The Board continues to approve any new commercial offering that involves the use of traffic or message data. A new commercial offering is a product or service that introduces a new capability that fulfils a purpose not yet covered before, e.g. the Daily Validation Report approved in ER 1150 (Sep 2016) reporting on payment activities on a daily level and maximum transaction amounts, or the gpi service and Tracker approved in ER 1153 (September 2016). The proposals will be presented to the relevant Board business committees for review, as per the current process.
4. The Board explicitly approves any new use of message data directly or indirectly **identifying ordering or beneficiary parties** (such as names, addresses, and account numbers) for inclusion in commercial offerings.
5. Swift will provide full **transparency** to make sure the community is informed and can verify at all times how their data is made available in Swift products and services. This information will be available on swift.com, in the user protected area.

Security and confidentiality

6. Swift will apply the required practices and processes to **guarantee data security and privacy, respect of regulations** and to ensure data is only used or accessed by authorized individuals or parties. Protecting message data is mission critical to Swift, as confidentiality of data touches upon the core of its activities.
   Swift will extract, process, and protect the data in accordance with all relevant policies and procedures, in particular:
   - Its internal **Security policies**, standards, and guidelines, including all relevant security measures in terms of data classification, data labelling, data distribution, data transmission, data storage, computer protection, data disposal.

- Its **privacy policies:** Swift will process the data in compliance with applicable data protection regulations, such as the General Data Protection Regulation (GDPR), and its own data protection policies with its customers, such as the Swift Personal Data Protection and Data Retrieval policies. Swift will implement all relevant appropriate safeguards (such as strict security measures, privacy impact assessments, limited retention periods and subsequent data purge, etc.) to protect the data.
- **Its controls on internal access**: Swift staff will only have access to data on a need-to-know basis, subject to clear rules on what they can do and not do, and after completion of adequate training on appropriate use and risks related to handling of that data. Access to data is currently authorised for internal market and service analysis, crisis simulation, product pricing, support, forensic analysis, account management purposes, or to demonstrate or market Swift's business intelligence solutions.

7. Swift will ensure not to share institution-specific data with other institutions and not to disclose commercially sensitive market volumes. When using data of the full community (e.g. for benchmarking purposes) Swift will always ensure that the aggregation is sufficient to avoid any direct or indirect identification of peers.

8. Swift will continue to apply its **124 days retention period** for full message data and delete it after this period.

Data Granularity

9. Expanding on ER 1161 on Payment Controls and ER1178 on Data Extraction of FIN Messages (which approved the access to full transaction details for 5 strategic initiatives), Swift may have access to full traffic and message data as required for point purposes and for statistical analysis for its own product development and technical optimization, in a highly secure and protected environment in Swift's EU OPC, on a permanent basis. The ability to test products and services using live production data is crucial to detect the variety of real live scenarios and local market practices (e.g. for the development of ISO 20022 translation rules).

   The results of such statistical analysis will be aggregated and anonymised and thus will not reveal the identity of Swift customers, individuals, other third parties, or their business relationships. Swift may use such results to improve its products and services and may share high level statistics regarding the research externally.

10. Swift manages the **evolution of its existing commercial data offering** and may include additional message data when in line with the intended purpose of the product or service as initially approved by the Board at the time of its launch, under the supervision and control of an internal data governance steering committee