

FATF Revised Recommendation 16 Guidance – Consultation Response

The industry association of Swiss debit card issuers “SwissDebitPay”, representing the interests of all major debit card issuers (banks), infrastructure service providers and ATM providers in Switzerland, provides the following comments on the public consultation regarding the Recommendation 16 Guidance, focussing on the aspects affecting the card and retail payment business.

1. Definition of cards and card numbers

SwissDebitPay welcomes the detailed definition of card products and card numbers. The clarifications that the card exemption applies regardless of initiation method (paragraph 182), that new digital card forms such as virtual cards fall within the definition of “card” (paragraph 183), and that tokenized card numbers are treated equivalently to traditional card numbers (paragraphs 196 and 198), together ensure a technology-neutral approach that supports innovation and financial inclusion.

2. Information request for cross-border ATM cash withdrawals

SwissDebitPay supports the objective to allow swift access to the identity of cardholders involved in cross-border cash withdrawals in case of suspicious activity or law enforcement investigations, and it agrees that a three-business-day timeframe for making that information available is appropriate. It cannot, however, support a mechanism under which a card issuer discloses a cardholder's name directly to an acquiring entity on that entity's own request. Without the involvement of the competent authority of the issuer's jurisdiction, the issuer has no way to verify the legitimate interest of the request and no control over further processing of cardholder's personal data once it has been disclosed – an outcome that falls short of the data protection standard that Chapter 9 of the draft Guidance itself sets out to achieve.

Under the proposed data flow, a private acquiring entity – which may be requesting information purely “on its own behalf”, with no competent authority involved at all – submits a request directly to the card issuer, and the issuer is expected to comply within three business days. SwissDebitPay considers this approach unsound for the following reasons.

First, the issuer cannot verify the legitimate interest underlying the acquirer's request. Paragraph 210 states only that “acquirers should indicate the purpose of their request,” but there is no mechanism by which the issuer – which has no independent knowledge of the transaction, the jurisdiction's suspicious activity indicators, or the investigation (if any) that gave rise to the request – can assess whether that stated purpose is genuine, proportionate, or lawful under the acquirer's or the issuer's domestic law. The model is, in effect, one of self-certification by the requesting party, with no independent gatekeeper. This falls short of the “lawfulness” principle, which requires that the collection, processing and transmission of personal data rest on a defined legal basis, not on an unverified assertion by a commercial counterparty.

Second, once the cardholder's name has been transmitted to the acquiring entity, the issuer has no control over, or visibility into, its subsequent handling. The acquirer may be located in a jurisdiction with a materially different – or materially weaker – DPP framework than the issuer's jurisdiction.

Recommendations

Paragraphs 208(b) and 210 shall be revised in a way that a request for cardholder information is always made to, and fulfilled through, the competent authority of the jurisdiction in which the card issuer is located, rather than directly between the acquiring entity and the issuer. Specifically:

- The acquiring entity (or, where applicable, the competent authority in the acquirer's jurisdiction acting on the acquirer's or a law enforcement authority's behalf) should submit its request, together with the stated purpose, to the competent authority of the issuer's jurisdiction – not directly to the issuer.
- The issuer's competent authority should verify that the request has an adequate legal basis and a legitimate AML/CFT or law enforcement purpose before any personal data is released.
- Once verified, the competent authority should either obtain the cardholder's name from the issuer and transmit it to the requesting party (directly, or via the competent authority in the acquirer's jurisdiction), or expressly authorise and supervise the issuer's direct disclosure to the acquirer, with a corresponding record retained by the competent authority.
- The existing three-business-day timeframe in paragraph 208(b) should be retained and should run from receipt of a verified request, so that the addition of a competent-authority gateway does not compromise the investigative usefulness of the mechanism.

3. Scope of card exemption

In general, card (and similar retail payment) transactions pose a low risk for money laundering and terrorist financing because the movement of funds and data occurs – governed by payment networks/schemes – between regulated entities that act on behalf of their respective customers and that conduct customer identification, customer due diligence and transaction monitoring for suspicious behaviour in accordance with FATF requirements. Each use of a card leaves a paper trail that can be traced back to the cardholder.

The exemption from information requirements for transactions involving the purchase of goods or services is comprehensible and well-founded in the context of card-based payments operating under a four-corner model and governed by a regulated payment network/scheme. However, linking the exemption from the information requirements to the existence of a “card” (in the broad sense described in paragraphs 183 and 193, including virtual cards, and in paragraphs 196 and 198 for tokenized card numbers) is in strong conflict with the principle of “same activity, same risk, same rules” invoked in the recommendation 16, when applied to digital wallets that are functionally equivalent to traditional cards. As described in Chapter 6.2 (paragraphs 192-193), it is the robust, standardised framework established by card networks – through their scheme rules, message protocols and security requirements – that underpins the low-risk profile of card transactions for the purchase of goods or services, not the mere formal existence of a “card”. The current practice of linking the exemption to a card rather than to the actual risk profile of the underlying (retail) payment instrument does not follow the principle of technology neutrality and undermines a level playing field in the market.



Recommendations

The “card exemption” should apply to all payment instruments (including certain mobile wallets) operating within regulated retail payment schemes that provide similarly robust and established scheme governance as traditional cards, ensuring an equivalent low-risk profile.

About SwissDebitPay

The industry association SwissDebitPay promotes cooperation between debit payment issuers in Switzerland, engages in non-competitive aspects of mutual interest; contributes to the process of shaping legal and regulatory developments; develops best practices for the industry; protects the integrity of debit payments; develops industry standards and coordinates other industry-wide initiatives (e.g. those aimed at innovation). Members of SwissDebitPay are the major Swiss debit card issuers, namely: UBS Switzerland AG, PostFinance AG, Raiffeisen, Zürcher Kantonalbank, Entris Banking AG, Migros Bank AG, SIX BBS AG, Viseca Payment Services SA, Berner Kantonalbank, Luzerner Kantonalbank Graubündner Kantonalbank, Schwyzer Kantonalbank, Zuger Kantonalbank, Banque Cantonale Fribourg, Bank, CIC (Schweiz) AG, Banca Popolare di Sondrio (SUISSE) SA, YAPEAL AG.

Contact

SwissDebitPay
Thomas Weber, Managing Director
c/o Kellerhals Carrard KIG
Rämistrasse 5, 8024 Zürich
+41 79 662 23 23
thomas.weber@swissdebitpay.ch