Newsletter of *GIF* of *SPU*

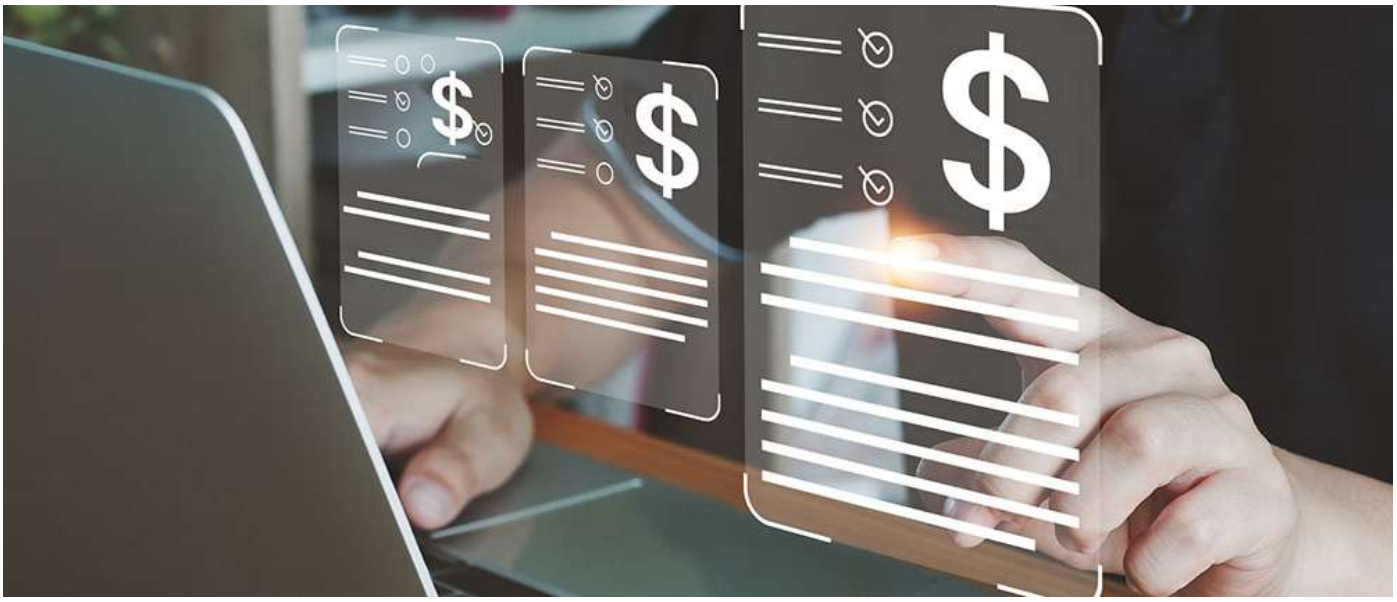
December 2025 Issue 34

Inside this Issue

Suspicious Transaction Reports Statistics (2025 January to June)

Number of STRs	2025 (Jan to Jun)	2024 (Jan to Jun)
From Financial Institutions and Insurance Companies	500 (19.9%)	556 (19.3%)
From Games of Fortune Operators	1,856 (73.8%)	2,181 (75.8%)
From Other Institutions	159 (6.3%)	142 (4.9%)
Total	2,515	2,879

- The total number of STRs received by the Financial Intelligence Office of the Unitary Police Service (*GIF* of *SPU*) during the first half of 2025 was 2,515, which represent a decrease of 12.6% as compared with the same period in 2024. The change was mainly due to the decrease in the number of STRs reported by the gaming sector.
- STRs received from the financial sector and gaming sector constituted 19.9% and 73.8% of total respectively, whereas those received from other institutions constituted 6.3%.



International Trend – Changes to Recommendation 16 on Payment Transparency

The Financial Action Task Force (FATF) has streamlined international requirements that will increase the safety and security of cross-border payments to better detect financial crimes. The changes to Recommendation 16 (R.16) of the FATF standard will ensure consistency of information required in payment messages to build a clearer picture of who is sending and receiving money, and help to eliminate fraud and error impacting account holders. Financial institutions are advised to take note of these changes as it may lead to greater compliance costs and operational changes, and be prepared to adapt these changes.

Background of Revision of FATF R.16

- The revision of FATF R.16 was prompted by rapid changes in the payment domain, including the variety of new products and services, technologies, business models, types of market participants, and the risks and vulnerabilities involved. The revision aims to keep FATF standards technology-neutral and **follow the principle of "same activity, same risk, same rules"**.
- The FATF intended to increase the **safety and security of cross-border payments**. These changes are designed to enhance the detection and prevention of financial crime.
- The revised standards aim to make the information accompanying payment messages more consistent, providing greater transparency of both originator and beneficiary, and help to **eliminate fraud and error that affect account holder**.
- The revision in FATF R.16 was also part of **the G20 Priority Action Plan** on making cross-border payments faster, cheaper and more transparent.

Key Changes of the Revised R.16

a. Structural Changes

- The new structure of revised R.16 differentiates the responsibilities and obligations for different types of payments or value transfers. Requirements based on types of activities rather than types of entities.
- Information should be structured, to the extent possible, in accordance with the established standards of the system used such as ISO 20022.

b. Clarification of Responsibilities in the Payment Chain

Payment chain new definition:

The payment chain starts with the financial institution **receiving the instruction** from the customer and ends with the financial institution servicing the beneficiary's account or providing cash to beneficiary. This "instruction route" brings clarity to responsibilities in complex, multi-party payment chains. It ensures that information travels end-to-end and is not fragmented.

c. Information Requirements

Cross-border Payments and value transfers

Cross-border Payments and value transfers		
	Above the *de minimis* threshold (higher than USD/EUR 1,000)	**Below the *de minimis* threshold** (no higher than USD/EUR 1,000)
Originator's Information	Must include name, account number*, address (or country and town), **date of birth (year-only as fallback, for natural person)**, and **Bank Identifier Code/Legal Entity Identifier/unique official identifier (for legal person)**.	Must include name and account number*.
Beneficiary's Information	Must include name, account number, country and town only (not full address).	Must include name and account number*.
Verification	- Originator information **must be verified by ordering financial institutions**. - **Identity of the beneficiary should be verified by beneficiary financial institutions**.	The abovementioned information **need not be verified for accuracy**, unless there is a suspicion of money laundering or terrorist financing.

*Note: For account number, where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included, which permits the traceability of the transaction.

Domestic Payments and value transfers

Domestic Payments and value transfers		
	Above the *de minimis* threshold (higher than USD/EUR 1,000)	**Below the *de minimis* threshold** (no higher than USD/EUR 1,000)
Originator's Information	Same requirements with cross-border payments and value transfers, unless the information can be made available to the beneficiary financial institution.	Must include name and account number of originator, or a unique transaction reference number which will permit the transaction to be traced back to the originator or the beneficiary.
Verification	---	The abovementioned information **need not be verified for accuracy**, unless there is a suspicion of money laundering or terrorist financing.

Card Payments

- **Purchase of goods and services**: Transaction carried out using a credit/debit or prepaid card for the purchase of goods and services (refers to purchases from individuals/entities who are onboarded by the relevant financial institution to accept card payments following the required customer due diligence), continue to be exempt from full R.16 requirements. The credit/debit or prepaid card number should accompany all transfers flowing from the transaction. **The name and location of the card issuing and merchant acquiring financial institutions should be made available upon request**.
- **Person-to-Person Transfer**: When a credit/debit or prepaid card is used for other types of payment or value transfer, e.g. Person-to-person transfer, **the transaction is subject to requirements above for domestic/cross-border payment or value transfers**.

Cash Withdrawals

For cross-border cash withdrawals using credit/debit or prepaid card, the **card number** should accompany cash withdrawal, while the **name of the cardholder** must be made available to the acquiring financial institution upon request within 3 business days of receiving the request.

Exemption for financial institution-to-financial institution transfers, net settlement and batched transactions

No information required for financial institution to financial institution transfer, and intermediary financial institutions do not have to unbundle net settlements carried out on behalf of customers, but the underlying transactions are still subject to R.16 requirements.

d. Responsibility of beneficiary financial institutions

Financial institutions are now required to **use technological tools** to protect against fraud and errors, such as recipient information verification systems.

For cross-border payments or value transfers above the *de minimis* threshold, the information received about the intended beneficiary should help the beneficiary's financial institution to monitor transactions, with the aim of identifying misdirected payments (e.g. due to possible money laundering, fraud or error). Beneficiary financial institutions should take measures to mitigate the risk of transfers being made to the wrong beneficiary, thus the financial institution should include at least one of the following (a), (b), or (c) measures:

(a) The beneficiary financial institution should check the extent of each transaction including the name and account number of the beneficiary in the **payment message aligns with the information held by the beneficiary financial institution**; or

(b) the beneficiary financial institution should conduct full **ongoing monitoring** to identify abnormal accounts, transactions, and activity, including misaligned beneficiary information, following a risk-based approach; or

(c) If the beneficiary and ordering financial institutions both participate in a pre-validation mechanism such as confirmation/verification of payee to check, for each transaction, that the name and account number of the beneficiary in the payment message aligns with the information held by the beneficiary financial institution, then this pre-validation may be used instead of (a) or (b) above.

Implementation Timeline and Next Steps

- The changes to R.16 were agreed by FATF members at the June 2025 Plenary.
- The changes of R.16 will come into effect **by the end of 2030**, allowing sufficient time for adaptation.
- The FATF will develop **additional guidance** and maintain ongoing engagement with the private sector to support preparation and smooth transition for the new requirements.

Conclusion

The changes to FATF R.16 represent a major international initiative to make cross-border payments **safer, more transparent, and more resilient against financial crime and fraud**. By clarifying roles, standardizing data requirements, embracing new anti-fraud technologies, and providing clearer rules on card transactions, the FATF is adapting to the evolving global payments ecosystem while ensuring continued progress towards financial inclusion and efficiency. Therefore, financial institutions must stay vigilant for upcoming regulatory and market changes that may impact their operations.

Source: "*FATF updates Standards on Recommendation 16 on Payment Transparency*" (https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html)

Case Study

Cross-border cash withdrawals to conceal suspicious activity

Mr. X, resident in country A, opens one or more bank accounts in countries B and C. When opening the account, Mr. X stated that the purpose of opening the account was savings and issued bank credit/debit cards. Shortly after the account was opened, Mr. X's account had frequent large cash deposits. Mr. X used his credit/debit cards issued in countries B and C to make frequent large cash withdrawals at ATMs in his home country A. Investigations from financial institutions in countries B and C revealed that there were multiple unknown individuals carried out cardless deposit transactions to Mr. X's account at the ATM.

The financial institution in Country A identified several of its ATMs had frequent abnormal cash withdrawal transactions. It was believed that the local financial system was abused for frequent cross-border withdrawal transactions at ATMs in Country A by using several credit/debit cards issued by financial institutions in Countries B and C. Its purpose was to conceal the actual source of the funds and might involved illegal activities. According to current R.16 rules, financial institutions in Country A can obtain the card issuing bank and jurisdiction through the bank card BIN code, but cannot obtain any information about the identity of the cardholder. Cardholder information is available only to the issuing financial institutions in countries B and C and information about Mr. X's activity is fragmented. As a result, Mr. X could circumvent domestic AML/CFT controls by financial institutions and law enforcement agencies in country A. The lack of transparency also hinders the detection and report of suspicious activities.

After the revision of R.16, for cross-border cash withdrawals using credit/debit or prepaid card, the card number should accompany cash withdrawal, while the name of the cardholder must be made available to the acquiring financial institution upon request within 3 business days of receiving the request.

Red Flags

- Frequent and large cash deposits shortly after account opened;
- The card issuing financial institution is unable to verify the identity of the depositor involved in the cash transactions and the reasons for cross-border cash transactions are unknown, there is possibility of using money-mule accounts;
- The acquiring financial institution is unable to obtain any information about the identity of cardholder, making it difficult to determine whether the credit cards were stolen or illegally used for cash withdrawal;
- All transactions conducted through ATMs, utilizing non face-to-face transaction to avoid customer due diligence carried out by financial institutions.

Recommendations

- For non-local customer onboarding, financial institutions should conduct adequate customer due diligence especially on customer's identity, the purpose for the account opening and transaction, and the source of funds.
- Enhanced customer due diligence measures should be implemented to determine the legitimacy of transactions, in particular when non face-to-face transactions are involved.
- Financial institutions should enhance monitoring measures to detect unusual transactions.

Contact us

Published in Dec 2025 **Published by:** **Financial Intelligence Office,** **Unitary Police Service,** **Macao Special Administrative Region Government**	Address: Avenida Dr. Mário Soares Nos. 307-323, Edificio "Banco da China", 22º andar, Macau	Tel: (853) 2852 3666 Fax: (853) 2852 3777 E-mail: info@gif.gov.mo Website: http://www.spu.gov.mo http://www.gif.gov.mo

If you have any suggestions and enquiries on this newsletter, please feel free to contact *GIF* of *SPU*.