Financial Economics Insights

Article

Regulatory Bypass and Look-Through Governance of Cross-Border U.S. Dollar Stablecoin Flows: A Fiat On- and Off-Ramp Approach

Meng Zhang[1,*]

[1] School of Law, Beijing Foreign Studies University, Beijing, China
* Correspondence: Meng Zhang, School of Law, Beijing Foreign Studies University, Beijing, China

Abstract: Dollar stablecoins can transfer value across borders while detaching account-based identity and reporting data from the blockchain leg. Focusing on privately issued, fiat-backed dollar stablecoins that reach a China-facing fiat interface, this article defines regulatory bypass as a break in information continuity across the account-address-account sequence. The ledger can reveal a transaction path, and prohibition supplies the legal boundary, but intervention still requires proof of customer identity, wallet control, transaction purpose and conversion function. International standards assign duties by function and preserve originator, beneficiary, custody and transaction data across regulated segments, but gaps persist at self-hosted wallets, offshore providers and in the evidentiary use of blockchain analytics. The proposed framework allocates duties according to transaction control and information access. Banks and payment institutions investigate identifiable fiat links; converters and facilitators answer for the functions they perform; platforms, custodians and issuers preserve records within their control through lawful cross-border channels. A reviewable interface record should connect account data, wallet-control evidence, transaction hashes, conversion terms and corroborating off-chain material. Risk signals may trigger inquiry, but restrictions, freezing, liability or referral require progressively stronger corroboration and legally authorised procedures. This reconstructs regulatory continuity without treating technical traceability as proof by itself.

Keywords: dollar stablecoins; fiat on- and off-ramps; regulatory bypass; look-through governance; blockchain analytics; anti-money laundering

Received: 07 June 2026
Revised: 27 July 2026
Accepted: 11 August 2026
Published: 14 August 2026

1. Introduction

An ordinary cross-border bank payment carries regulatory information with the money: a named customer, account relationship, counterparty, amount, purpose, and reviewable records. A dollar stablecoin can separate that information from the value. A customer may fund an exchange or dealer from a Chinese bank account, receive tokens at a blockchain address, move them through self-hosted (or unhosted) wallets, and cash out through another platform, broker, or payment account. The ledger preserves addresses, amounts, timestamps, and transaction paths, yet the controller's identity, residence, beneficial ownership, source of funds, and economic purpose depend on off-chain data. Reuter describes this condition as pseudonymity: transactions are public, while wallet addresses do not directly disclose personal or geographic information [1]. The relevant object is the account-address-account sequence and the fiat on- and off-ramps through which balances pass between stablecoins and the existing financial system [2]. The analysis concerns privately issued, dollar-denominated or dollar-pegged stablecoins backed mainly by cash, bank deposits, or short-term liquid assets [3]. Its legal focus is the transaction path that touches a China-facing fiat interface.

China's account rules supply the baseline. Financial institutions must identify customers and beneficial owners, understand transaction purpose, examine source and

use of funds in higher-risk cases, monitor activity, and keep records sufficient to reconstruct each transaction (Anti-Money Laundering Law of the People's Republic of China, 2024 Revision [hereinafter AML Law]; Measures for the Administration of Customer Due Diligence and the Preservation of Customer Identity Information and Transaction Records by Financial Institutions, PBOC et al. Order [2025] No. 11, arts. 3--4, 7 [hereinafter CDD Measures]). Cross-border bank reporting also captures payer and payee data, currency, amount, counterparty jurisdiction, transaction code, and narrative (Measures on the Collection of Statistics and Declaration of the Balance of Payments, 2013 Revision; Detailed Rules for the Implementation of the Declaration of Balance of Payments Statistics through Banks, Hui Fa [2022] No. 22, art. 7 [hereinafter BOP Detailed Rules]).

Once value leaves this environment, the regulatory picture becomes uneven. FATF notes that peer-to-peer transfers between self-hosted wallets may proceed without an AML/CFT-obliged intermediary, while non-compliant OTC brokers and peer-to-peer platforms can provide cash-out routes outside formal controls [4]. Travel Rule data and suspicious-transaction reporting then cover only the parts of the chain that pass through an obliged entity. Public visibility offers a transaction trail, though attribution often depends on exchange records, device or account data, behavioural inference, and blockchain-analytics labels that require verification. Cross-country evidence points in the same direction: foreign-exchange account and cross-border restrictions that reduce deposit dollarisation show no statistically significant effect on gross stablecoin inflows in the available sample [5].

China's 2026 Notice supplies the prohibition-based legal boundary. It treats Tether and comparable virtual currencies as lacking legal-tender status, prohibits virtual-currency exchange and related financial activities in China, bars overseas actors from illegally serving domestic subjects, and prevents financial institutions and non-bank payment institutions from providing account opening, fund transfer, clearing or settlement services for those activities (Notice on Further Preventing and Disposing of Risks Relating to Virtual Currencies and Related Activities, Yin Fa [2026] No. 42, items (1) and (6) [hereinafter 2026 Notice]). Difficult cases arise when the transaction is divided among actors holding different pieces of information: the bank sees a fiat payment, an intermediary arranges conversion, and an offshore platform retains customer and wallet records. Existing work explains peg maintenance through arbitrage [6], places stablecoins within debates over private money and financial regulation [7,8], and develops functional oversight, data access, and cross-border cooperation [9]. The unresolved issue is narrower: at a fiat interface governed by a prohibition, which records must be recovered, who can lawfully obtain them, and what evidence can support reporting, rejection, freezing or referral? "Regulatory bypass" refers to this break in information continuity. Value reaches or leaves the account system, while identity, transaction background, reporting fields, and the customer's connection to relevant wallets cannot be established from the records available to the regulated institution. This is a structural description of missing information, not a presumption that every user intended to evade regulation.

The central claim is that enforcement at fiat interfaces should rebuild a verifiable link among the customer, the fiat account, wallet control and the on-chain path relevant to conversion. A prohibition defines the legal boundary; its practical effect depends on whether institutions can recognise the stablecoin connection and record the grounds for intervention. Look-through governance should therefore assign duties according to control over the transaction and access to information. Banks and payment institutions can apply risk-based due diligence to identifiable fiat links, seek records supporting source and purpose, preserve wallet addresses and transaction hashes, and report unexplained patterns. Commercial converters, OTC brokers and domestic facilitators should answer for the exchange, matching, collection or payment functions they actually perform. Records held by offshore platforms, custodians and issuers should be obtained through lawful cooperation or production mechanisms once a legally sufficient China-facing connection is established. Blockchain analytics can support screening and reconstruction; consequential measures require corroboration from account records,

customer files, communications, device data or the payment's commercial context. This approach applies the FSB principle of "same activity, same risk, same regulation" within China's prohibition-based policy [9].

The contribution is to organise the problem around information continuity, locate duties where fiat and stablecoin systems meet, and separate risk signals from evidence sufficient for coercive action. Section 2 maps the partial records held at each account and address layer. Section 3 tests how international standards preserve transaction information and identifies the remaining host-state, self-custody and evidentiary gaps. Section 4 translates those gaps into China-facing duties, minimum data fields, corroboration requirements and proportionate measures.

2. Regulatory Continuity and Its Breakdown

Seen in those terms, the legally relevant sequence can be reduced to three legs: entry of fiat funds, transfer of the stablecoin, and return to fiat. CPMI defines on- and off-ramps as the entities or payment systems through which a stablecoin is converted into or out of sovereign currency and balances move between the stablecoin arrangement and the existing financial system [2]. In a China-facing transaction, the entry leg may begin when a customer instructs a bank or non-bank payment institution to pay an offshore exchange, a domestic collector, an OTC dealer, or a third party nominated by one of them. The customer then receives stablecoins in a hosted account or at a self-hosted address. The tokens may remain within the exchange's internal ledger, move to another exchange, or pass through one or more self-hosted wallets before reaching an exit provider. The final provider sells the tokens, arranges an offsetting payment, or withdraws fiat to a bank or payment account. Reuter's transaction map captures an important asymmetry: the initial fiat deposit and the later disposition of fiat occur in the banking system and are absent from blockchain data, whereas transfers between exchanges and self-hosted wallets are generally visible on chain; transfers between customers on the same exchange may leave no public-chain record [1]. The point of legal reconstruction is therefore to identify the information available at each interface.

A Chinese bank or payment institution knows its customer, the sending or receiving account, the counterparty named in the payment message, the amount and time, and any transaction description produced by its own system. Customer due diligence must identify and reasonably verify the customer and beneficial owner, understand the purpose and nature of the relationship, examine source and use of funds where risk is higher, and preserve records sufficient to reconstruct each transaction (CDD Measures). Where a payment qualifies as a reportable external receipt or payment, the bank also collects payer and payee names, identifiers, currency, amount, counterparty jurisdiction, a balance-of-payments transaction code, and a narrative supplied by the reporting subject (BOP Detailed Rules, arts. 4, 6--7).

An exchange or OTC converter usually sees a different file: customer onboarding material, the fiat order, the token and quantity, the price, the destination or source address, and the transaction hash. A custodial wallet may control the private keys and suspend a transfer; a self-hosted wallet leaves control with the user. The issuer can observe transfers in its token and may retain smart-contract powers to blacklist, freeze, or burn balances, while retail identity is generally available only where the holder or intermediary has a direct account relationship. FATF's account of the ecosystem accordingly distinguishes issuers, exchanges, custodial intermediaries, payment service providers, unhosted wallets, and analytics firms by the functions they actually perform [4]. The same payment chain is visible in several partial records, with no record naturally containing all of them.

Regulatory continuity breaks once the address layer is expected to carry information that account systems normally generate. The identity break appears because a public address identifies a cryptographic destination, not the natural or legal person who controls it. Reuter describes blockchain records as pseudonymized: the ledger records sender and receiver addresses, while names and residence must be supplied from elsewhere [1]. An address may belong to an individual, an exchange omnibus wallet, a

custodial service, or an OTC dealer; one user may rotate addresses, and one service may aggregate many users. Attribution requires a bridge from on-chain facts to exchange onboarding files, bank-account ownership, device or login information, communications, proof of control, or a verified response from a service provider. Analytics can cluster addresses and attach risk labels, yet FATF notes that providers use different taxonomies, making outputs difficult to compare [4]. A label can justify inquiry. It cannot by itself establish beneficial ownership, residence, or participation in a prohibited service.

The transaction-context break is broader. A transfer record shows the token, amount, addresses, time, and path, but gives no transaction purpose, economic beneficiary, residence, source of fiat funds, or basis for classifying the payment as trade, investment, remittance, evasion, or another activity. Account-based controls are designed to generate those facts. Chinese financial institutions must understand transaction purpose and, where risk is higher, source and use of funds; they must also perform manual analysis, record the reasons for reporting or exclusion, and verify the conclusion against customer due diligence (Measures for the Administration of Financial Institutions' Reporting of Large-Value Transactions and Suspicious Transactions, art. 14, as amended by PBOC Order [2025] No. 10 [hereinafter Reporting Measures]). Balance-of-payments reporting places a payment within a resident/non-resident relationship and adds a transaction code and narrative (BOP Detailed Rules, arts. 4--7). A self-hosted transfer triggers none of these steps by itself. FATF defines a peer-to-peer transfer as one conducted without a VASP or other obliged entity and observes that no intermediary then performs customer due diligence or suspicious-transaction reporting [10]. Public-ledger visibility still assists tracing when combined with other sources, while limits in coverage, timeliness, accuracy, and reliability constrain analytics-based conclusions [10]. The break may also be created by the conversion arrangement.

A customer can pay a domestic collector while an offshore platform records the token order; at exit, fiat may arrive from an unrelated individual or payment processor. The bank can review the account entry and the platform can review the token transfer, yet neither record supplies the correspondence between them. Responsibility fragments in the same way. Banks hold reliable account and customer data but usually lack the customer-to-wallet link. Exchanges and custodial wallets may hold that link and the order history, though the entity may be offshore. Issuers can see token movements and may control specified addresses, while secondary-market identity and residence usually remain outside their customer files. Analytics firms see transaction graphs without the records needed to prove wallet control. Informal OTC operators may know the commercial arrangement but preserve little documentation. FATF identifies cross-border gaps in customer and transaction information, together with uncertainty over the person subject to duties and the jurisdiction responsible for supervision [10]. No participant naturally holds the complete account-address-account history.

These discontinuities define regulatory bypass as an evidentiary condition. Value can leave the account pathway for one or more legs and later re-enter a regulated account, while application of the 2026 Notice still turns on proof linking the customer, payment and wallet to a covered exchange, intermediation, collection or settlement function (2026 Notice, items (1) and (6)). A bank transfer displaying an unusual counterparty or an address carrying a risk label can justify inquiry and monitoring. Reporting, restriction, liability or referral requires corroborated facts concerning conversion, agency, matching, collection, payment or another covered function.

The same functional inquiry dispels the idea that stablecoin circulation has removed intermediaries. Fiat-backed stablecoins are issued and redeemed through identifiable organisations, distributed and traded through exchanges and dealers, held through custodial or self-hosted wallets, and commonly returned to fiat through an intermediary [3]. Lyons and Viswanath-Natraj's account of Tether shows direct dealings between private investors and the issuing treasury, together with exchange-based distribution and arbitrage [6]. FATF likewise treats an issuer as an obliged entity when it conducts exchange or transfer for customers and treats exchanges, custodial wallet providers and

OTC brokers as service providers when they exchange, transfer, safeguard or administer stablecoins for or on behalf of others [4]. A provider of wallet software or other ancillary infrastructure remains outside that category where it neither controls assets nor actively facilitates a covered service [4,10]. Interface duties should follow that allocation of functions.

A bank or payment institution can be required to understand its customer's fiat transaction, investigate an identifiable stablecoin connection, obtain records reasonably available from the customer, and preserve the basis for reporting, rejection or continued service. A converter, exchange or custodial wallet should bind the customer to the relevant account or wallet, retain the order and transaction hash, and provide records through the legal process applicable to it. An issuer's duties may extend to address-level controls that it actually possesses, subject to lawful authority and a sufficiently identified transaction. Their combined obligations should reach the portion of the chain needed to explain the conversion under review, together with enough corroboration to establish wallet control and transaction context. The remaining public-ledger history falls outside the assigned duty. Remote historical transfers, analytics labels with an undisclosed basis, and links resting only on common exposure to a service should remain risk indicators. This boundary gives interface regulation a determinate object: the connection among a customer, a fiat payment, a controlled or attributed wallet, and the stablecoin transfer that completed the conversion. The next question is how far international standards preserve and transmit those links, and where host-state connection, self-hosted wallets and evidentiary thresholds still interrupt them.

3. International Standards and the Residual Interface Gap

The international baseline begins with the FSB's global-stablecoin recommendations, which organise supervision around economic functions and the principle of "same activity, same risk, same regulation." Authorities are expected to identify the persons responsible for issuance, transfer, custody, trading, user access and other material functions; bring critical intermediaries within the regulatory perimeter; and apply requirements proportionate to the risks and control exercised. Recommendation 6 adds the information component: stablecoin arrangements should collect, store, safeguard and report data through robust systems, while authorities should obtain timely and complete access to relevant on-chain and off-chain information wherever it is located. Recommendation 3 calls for cross-border communication, information sharing and consultation, and Recommendation 10 expects an arrangement to satisfy each jurisdiction's applicable requirements before operating there [9]. The IMF-FSB synthesis places these rules within a wider policy baseline. Licensing or registration of issuers and service providers, together with reporting requirements, can reduce data gaps and support financial-integrity and capital-flow measures; the same framework leaves jurisdictions room to adopt additional measures suited to local risks [11]. The FSB concentrates on financial-stability outcomes and relies on FATF, CPMI and other sectoral standards for anti-money-laundering, payment and market-infrastructure obligations. The IMF adds a macro-financial reason for preserving interface data: stablecoin issuers generally lack direct visibility into the residence or nationality of secondary-market holders, which limits cross-border statistics and policy assessment [3].

These standards already resolve an important perimeter question for the account-address-account sequence. Responsibility follows the financial function and the institution's practical capacity to control assets, execute a transaction, bind a customer to a wallet, or retain data. A trading platform that converts fiat, executes transfers and holds customer assets falls within the perimeter for those functions. A custodian answers for private-key control and transaction records. An issuer that performs customer-facing exchange or transfer services may carry corresponding obligations, while software developers and infrastructure providers remain outside the perimeter when their role is limited to ancillary technology. This functional allocation also limits the expected reach of each participant: data access should cover the part of the chain necessary for effective

supervision, without turning every provider into the repository of a user's entire blockchain history.

Cross-border implementation remains incomplete. The FSB's 2025 peer review found few completed global-stablecoin frameworks, material differences in reporting requirements, limited use of supervisory data and fragmented cooperation mechanisms. Reporting content and frequency vary, data reported by regulated firms remain incomplete, and many authorities rely on commercial providers for information not otherwise available [12]. Uneven implementation leaves room for regulatory arbitrage. The regulatory direction and responsible actors are clear; practical effect still depends on domestic connecting rules, enforceable production powers and interoperable records.

The FATF and CPMI supply more specific rules for transaction information at the fiat interfaces. FATF Recommendations 10 and 11 require customer and beneficial-owner identification, an understanding of the purpose and intended nature of the relationship, ongoing scrutiny, and records sufficient to reconstruct individual transactions. Recommendation 15 requires virtual asset service providers (VASPs) to be regulated, licensed or registered and effectively supervised. Recommendation 16 requires accurate originator and beneficiary information to remain with a payment or value transfer throughout the payment chain, enabling receiving and intermediary institutions to detect missing fields and take appropriate measures [13]. The 2021 FATF guidance applies these duties through a broad, technology-neutral VASP definition covering exchange between virtual assets and fiat currency, exchange between virtual assets, transfer, safekeeping or administration, and specified financial services connected with issuance. A provider need not perform every leg of an exchange to fall within the definition; active facilitation as a business for or on behalf of another person is sufficient. Custodial wallets and commercial over-the-counter brokers can therefore carry customer-due-diligence, record-keeping, suspicious-transaction-reporting and Travel Rule duties. A user controlling their own keys, a software supplier providing a self-hosted wallet application, or a network validator performing only technical functions ordinarily falls outside that category [10].

CPMI's account of cross-border stablecoin payments places these duties in an end-to-end sequence of obtaining the stablecoin, transferring it, converting it and crediting the recipient. Its definition of on- and off-ramps captures the entities or payment systems through which sovereign currency and stablecoin balances move between the arrangement and the existing financial system [2]. Together, the rules assign duties to actors that meet the customer, execute conversion, control assets or possess transaction information; the blockchain network carries no institutional duty of customer identification. The European Union demonstrates how this baseline can be translated into interface rules. Crypto-asset service providers must obtain, hold and transmit originator and beneficiary information across originator, beneficiary and intermediary service providers (Regulation (EU) 2023/1113, arts. 14, 16 and 19--21). They must also identify transfers involving self-hosted addresses and, for transfers above EUR 1,000, verify ownership or control (Regulation (EU) 2023/1113, arts. 14(5) and 16(2)). The EBA Guidelines add workable methods, including a predefined transfer, digital signature, remote verification and combinations of methods where one method lacks sufficient reliability. They also structure a risk-based choice among execution, rejection, return or suspension, with reasons documented where a deficient transfer is executed (European Banking Authority, Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113, EBA/GL/2024/11, paras. 9, 21--31, 52--64 and 76--90 [hereinafter Travel Rule Guidelines]). Their definition of the transfer chain as the end-to-end sequence from originator to beneficiary makes information continuity an operational requirement. Messaging systems should transmit required fields without gaps or errors, maintain data integrity when formats change, and use secure alternative channels where the on-chain message cannot carry the full dataset. Missing information alone does not establish suspicion, and transfers involving a crypto-asset service provider remain distinguishable from person-to-person transfers conducted without one (Travel Rule Guidelines, paras. 52--53;

Regulation (EU) 2023/1113, art. 2(4)). The FATF's 2025 implementation review nevertheless records continuing difficulty in identifying unlicensed providers, mitigating offshore VASP risk and operationalising the Travel Rule across jurisdictions [14]. Legal adoption is only a starting point: a rule becomes effective only when counterparties can exchange compatible data, supervisors can identify the provider behind a transfer, and missing information produces a recorded response. The framework preserves identity and transaction fields across regulated segments; a segment with no obliged entity remains outside that information chain.

The residual gap appears where the cross-border sequence reaches a host state, passes through self-hosted wallets, or produces legal consequences from analytical inferences. A foreign-issued stablecoin may acquire a large local footprint before it becomes systemically important in its home jurisdiction, leaving the host authority without direct supervisory powers over the issuer, platform or custodian. The FSB identifies this asymmetry expressly and relates it to data gaps and limited host-state supervisory and enforcement capacity [15]. FATF guidance notes that a jurisdiction may choose to require registration for services directed to local residents and identifies targeted advertising, local-language interfaces, offices, servers, distribution networks and customer-facing operations as possible indicators; that extension remains a domestic choice. MiCA offers one implementation model by treating active solicitation, promotion or advertising by a third-country firm as conduct outside the client's "own exclusive initiative" (Regulation (EU) 2023/1114, art. 61). China's 2026 Notice prohibits overseas entities from illegally providing virtual-currency services to domestic subjects and bars domestic financial institutions and payment institutions from supporting the prohibited activities (2026 Notice, items (1) and (6)). International standards and the Notice leave the China-facing connection test to domestic law, which must evaluate targeting, recurring access, local facilitation and fiat settlement together. These factors are possible inputs to a domestic connecting rule; they do not themselves establish Chinese jurisdiction.

The problem reflects the wider implementation limits of international financial soft law: common standards can coordinate objectives and vocabulary, while legal authority, jurisdiction and enforcement continue to depend on national measures [16]. Stablecoin scholarship has accordingly treated compliance with multiple national regimes and international enforceability as central sources of fragmentation [17].

The Travel Rule's institutional design leaves another discontinuity. FATF defines peer-to-peer transfers as transfers without a VASP or another obliged entity. No intermediary then performs customer due diligence, transmits originator and beneficiary information or files a suspicious-transaction report. FATF's 2026 targeted report accordingly treats P2P transfers through self-hosted wallets as a central vulnerability and directs risk mitigation toward issuers, VASPs and regulated institutions when those actors later encounter the transaction [4]. Public-ledger visibility supplies a transaction path, and regulated entry or exit providers can obtain information from their own customer, assess self-hosted wallet risk and seek proof of control. It does not create a continuous identity record between two self-hosted addresses [4].

The evidentiary problem runs deeper. International materials encourage blockchain analytics for transaction monitoring, sanctions screening and identification of high-risk exposure; official guidance also recognises that such tools may not identify the underlying owner without off-chain verification (New York State Department of Financial Services, Guidance on Use of Blockchain Analytics, 28 April 2022). Clustering heuristics can merge unrelated actors, attribution tags can be false or ambiguous, and their evidential value depends on provenance, disclosed methodology, reproducibility and a reviewable chain of evidence [18]. International standards do not establish a uniform threshold connecting an address label or transaction graph to account restriction, administrative liability or criminal referral, nor do they prescribe a common procedure for notice, challenge and correction. They also leave unresolved how a regulated institution should document confidence levels, disclose the basis of a vendor-generated label, respond to a corrected attribution, and distinguish a direct transaction with a risky service from several remote

hops in a longer chain. The remaining task is to translate the international baseline into China-facing interface duties, minimum data fields, corroboration requirements and proportionate, reviewable measures.

4. Reconstructing Continuity at China-Facing Fiat Interfaces

China's implementation problem begins when an account institution must decide whether an otherwise ordinary payment is connected to a stablecoin conversion. The 2026 Notice prohibits domestic fiat-to-virtual-currency exchange and related services, bars unlawful overseas provision to domestic subjects, and prevents banks and non-bank payment institutions from supplying account, transfer, clearing or settlement support (2026 Notice, items (1) and (6)). Item (5) separately requires data-based monitoring, information sharing and cross-verification (2026 Notice, item (5)). Existing account rules supply the operating standard. Financial institutions must reassess a customer when transactions depart from the known identity, business need or risk profile; higher-risk cases permit inquiries into purpose, source and use of funds, closer monitoring and reasonable limits on transaction method, scale, frequency or service type (CDD Measures, arts. 25--28). The Reporting Measures require manual analysis and a recorded explanation both when a case is reported and when it is excluded (Reporting Measures, art. 14). The resulting threshold is a recognisable stablecoin connection established through mutually consistent facts. These may include payment to a verified exchange, converter or collector; a customer-provided platform order, wallet address or transaction hash; repeated transfers to changing personal accounts followed by receipt of a fixed quantity of dollar stablecoins; rapid inbound payments from unrelated persons consistent with an off-ramp; or device, communication and pricing evidence that connects the fiat and token legs.

A single vendor label, generic payment narrative, contact with a person who also trades virtual currency, or several remote on-chain hops from a risky service has substantially less weight. Those facts justify inquiry and preservation; prohibited activity requires a further evidential link among the customer, the fiat payment and the relevant conversion. This calibrated use of look-through analysis accords with the Chinese financial-law account of "substance over form," while retaining the boundary that administrative discretion should not expand merely because transactions can be technically traced [19,20]. For a bank or payment institution, the resulting duty remains tied to its customer and its fiat record.

It may request the order or agreement underlying the payment, the apparent converter, evidence of source and purpose, the stablecoin type and amount, the relevant chain, wallet address and transaction hash, and proof that the customer controls or transacted with the address. It should preserve the explanation, materials checked, manual analysis and grounds for reporting, restricting or continuing the service. Where the fiat leg is genuinely an external receipt or payment, the reporting subject and bank must state its true economic nature and supply the counterparty jurisdiction, transaction code and narrative required by the balance-of-payments rules (BOP Detailed Rules; Guidelines for the Declaration of Balance of Payments Statistics through Banks (2023 Edition), Hui Fa [2023] No. 10, pt. I(A)(5)). Balance-of-payments reporting follows the actual resident--non-resident or other specified external transaction. A payment to a domestic collector does not enter that reporting system merely because an offshore platform records the corresponding token order; the bank should retain the stablecoin connection in its AML file and correct any false description of the payment's purpose. Non-bank payment institutions carry the same interface logic through their duties to conduct continuing user due diligence, preserve payer and payee information in complete and traceable payment instructions, monitor abnormal accounts and keep user and transaction records (Regulations on Supervision and Administration of Non-bank Payment Institutions, State Council Decree No. 768, arts. 18, 21, 23, 25 and 31).

Commercial OTC converters and domestic facilitators require a functional assessment because they may hold the missing correspondence between the fiat and token legs. Repeated customer-facing service, negotiated rates or fees, systematic matching,

nominated collection accounts, control over customer funds and coordinated release of stablecoins indicate exchange, matching, collection or payment as a business. Classification follows the performed function despite the use of a personal account, a "consulting" description or a technology-service contract. An isolated disposal of one's own holdings without facilitation or remuneration supplies a weaker basis for classification as a commercial intermediary. FATF's functional definition reaches exchanges, custodial wallets and OTC brokers when they conduct exchange, transfer, safekeeping or administration for or on behalf of another person, while ancillary software remains outside that perimeter [4,10].

The same distinction should govern domestic assistance: liability requires knowledge or constructive knowledge of the offshore illegality, and its scope should follow the conversion, custody, matching or payment actually performed and the information reasonably available for that function (2026 Notice, item (18)). An offshore platform acquires a China-facing connection when the overall record shows purposeful and repeated service to domestic subjects, such as Chinese-language solicitation directed to the market, domestic agents or collectors, onboarding that identifies Chinese residence, recurring settlement through Chinese accounts, or a distribution network arranging local fiat conversion. Mere technical accessibility has limited weight. FATF lists targeted communications, local-language interfaces, offices or servers, customer-facing operations and distribution networks as factors a jurisdiction may choose when defining a host-state connection [10]. Any China-facing production or preservation duty must then operate through a lawful domestic or cross-border mechanism rather than an assumed direct extraterritorial command.

Once that connection is established, China-facing obligations should be pursued through service restrictions, preservation and production requests, home-host supervisory cooperation and action against domestic facilitators. China-facing duties should remain confined to the information and control each offshore participant actually possesses. A platform or custodian can preserve onboarding, orders, wallet links, login and transfer records; an issuer can preserve token-level records and, where lawfully directed, use address controls within its smart contract. The issuer ordinarily cannot identify every secondary-market holder from the ledger alone [4]. Pure self-custody software likewise carries no institution-like duty when it neither controls private keys nor actively facilitates exchange, matching, settlement or redemption. If the same provider controls customer assets or a fiat gateway, the obligation attaches to that additional function.

Once the connection is concrete enough to justify inquiry, continuity depends on the content and evidential quality of the interface file. A usable record should join information already generated by the account system with a limited set of transaction-specific on-chain fields. The account side should identify the customer and beneficial owner, the paying or receiving account, the fiat counterparty, amount, currency, time, payment channel, stated purpose, source of funds where relevant, and any balance-of-payments code and narrative. The stablecoin side should record the token and network, contract address where needed to distinguish assets with the same symbol, sending and receiving addresses, transaction hash, block time, token amount, order number or exchange quotation, and the claimed relationship between the customer and each relevant address. Evidence of wallet control may consist of remote verification displaying the relevant address, a customer initiating a predefined transfer, signing a specific message, or using another reliable technical method (Travel Rule Guidelines, paras. 83--85). The chosen method should match the wallet type, technical setting and assessed risk, and the file should explain why it establishes control in that transaction. The correspondence field is especially important: it should state how the fiat amount, exchange rate, commission, order time and token transfer fit together, and identify any domestic collector, OTC broker, platform account or third-party payer between them.

The duty to obtain them arises only after identifiable facts have connected a fiat transfer to a possible purchase or cash-out, and remains limited to the materials needed

to explain that conversion. Financial institutions are already required to keep transaction data, vouchers, contracts, business correspondence and other materials in a form sufficient to reconstruct and trace each transaction for at least ten years (CDD Measures, arts. 42--44). The interface file gives that general duty a transaction-specific content. It should cover the portion of the path needed to explain the conversion, rather than demand the customer's entire wallet history. A risk label or transaction graph requires a separate metadata record.

At minimum, the institution should retain the vendor or public source, the date and version of the result, the address or cluster queried, the category assigned, whether exposure is direct or separated by intervening hops, the confidence or severity level, the principal methodology disclosed by the provider, and any later correction. The distance from the labelled service matters. A direct payment to a verified exchange deposit address carries a different inference from an address that interacted several transactions earlier with a cluster containing mixed lawful and unlawful activity. Vendor taxonomies also differ, and clustering rules can merge unrelated users or propagate a mistaken attribution across many addresses [18]. An immutable ledger assists with preservation of the transaction record; address control, off-chain label accuracy and transaction purpose still require separate proof. Chinese scholarship on blockchain evidence captures the same distinction by separating the strengthened authenticity of data after it is written to a chain from the continuing need to examine the source and truthfulness of data before entry [21]. The 2016 rules on electronic data accordingly require review of authenticity, legality and relevance, together with documentation of source, time, method, process and integrity checks (Provisions on Several Issues Concerning the Collection, Extraction, Examination and Judgment of Electronic Data in Handling Criminal Cases, Fa Fa [2016] No. 22, arts. 2, 14 and 22--24).

These principles support an evidential sequence suited to interface regulation. An address label, atypical payment pattern or incomplete explanation can trigger enhanced due diligence and manual review. A risk-management measure such as delayed execution, a limit on transaction type, refusal of a particular payment or a suspicious-transaction report requires a documented combination of account facts, customer materials and on-chain data. Administrative liability or criminal referral demands a fuller chain: proof of the customer's relationship to the fiat account, reliable attribution or control of the relevant wallet, correspondence between the fiat and token legs, and facts showing exchange, matching, collection, payment, agency or another prohibited function. Communications, device and login records, repeated pricing patterns, platform confirmations, counterparty records and verified responses from service providers can supply that corroboration. A transaction hash identifies a transaction recorded on the relevant ledger; it does not by itself prove the controller, beneficiary, purpose or conversion function. Beneficial ownership and knowing assistance require the corroborating links above, especially where exposure is remote and unexplained.

Data protection rules apply throughout the reconstruction. Public-chain information enters the personal-information regime when it is linked or reasonably linkable to an identified customer. Financial-account data are expressly sensitive, while linked transaction records may materially affect personal rights and therefore require commensurate safeguards. Processing can rest on the need to perform statutory AML and risk-control duties, yet it remains subject to a specific purpose, direct relevance, minimum scope, data quality and security (Personal Information Protection Law of the People's Republic of China, 2021, arts. 4--9, 13 and 28--30 [hereinafter PIPL]). Access should be role-based and logged; analytics results should be separated from verified facts; retention should follow the applicable financial-record period; and corrected labels or wallet attributions should be propagated to internal users and relevant recipients. Cross-border provision of customer, wallet or transaction data must use an available statutory mechanism and satisfy the applicable assessment, certification, standard-contract or other requirements, together with any exemptions and safeguards provided by the data-export rules (PIPL, arts. 38--41 and 55--56; Provisions on Facilitating and Regulating Cross-

Border Data Flow, CAC Order No. 16, arts. 3--8 and 10--11). These controls preserve the evidence needed for supervision while keeping open-ledger analysis within a defined, reviewable scope.

Information continuity has practical value only when the resulting measure is calibrated to the strength of the record and remains open to correction. The ordinary response to a weak but credible connection is additional monitoring or a focused request for materials. Repeated conversions, unexplained third-party collections, rapid in-and-out movement, use of multiple nominated accounts, direct exposure to a verified illicit service or facts suggesting commercial facilitation can support enhanced due diligence, shorter review cycles, management approval and reasonable limits on transaction mode, scale or frequency. Where required due diligence cannot be completed, the institution may not establish the relationship or provide the prescribed one-off service; for an existing relationship, it must terminate the relationship as appropriate and file a suspicious-transaction report (CDD Measures, art. 30). If enhanced due diligence shows that the risk still exceeds the institution's management capacity, it must refuse the business or terminate the relationship (CDD Measures, art. 28). A customer's refusal to cooperate with reasonable due diligence also permits, under prescribed procedures, restrictions, refusal or termination and, depending on the circumstances, a suspicious-transaction report (AML Law, art. 38). Chinese law constrains that discretion: measures must follow prescribed procedures, remain commensurate with the assessed risk, preserve basic necessary financial services and may not amount to an unlawful freeze (AML Law, arts. 4 and 30; CDD Measures, art. 28). The decision record should identify the triggering facts, materials requested and received, alternative explanations considered, analytical result, measure selected, responsible reviewer and date for reassessment. That discipline is particularly important where a commercial analytics score affects access to an account. The manual-analysis duty under the Reporting Measures, together with the explanation and refusal rights for solely automated decisions with major effects under the PIPL, requires a human judgment that tests vendor output against the full record (Reporting Measures, art. 14; PIPL, art. 24). A customer may challenge an AML risk-management measure; the institution must respond within fifteen days, basic necessary services require prompt handling, and the customer may complain to the AML authority or bring proceedings in court (AML Law, art. 39). Where applicable law permits details to be withheld temporarily because disclosure would prejudice an investigation, the institution should still record internally the factual basis, duration and reason for withholding, and complete review or notice when the impediment ends. Chinese analysis of financial regulatory measures reaches the same institutional conclusion: preventive action may require speed, while proportionality and an opportunity to be heard remain relevant once urgency recedes or the measure materially affects private interests [22].

Freezing requires a sharper separation of powers. A bank's contractual or AML risk controls can delay, refuse or limit a service within their legal scope; they do not confer a general power to freeze funds. Under the revised Anti-Money Laundering Law, where an AML investigation involves a customer transferring funds from the account under investigation, temporary freezing may be imposed only when the State Council's anti-money-laundering administrative authority considers it necessary and its responsible head approves it; the measure lasts no more than forty-eight hours and must be lifted absent a lawful continuation decision (AML Law, art. 45). An offshore platform or stablecoin issuer may have the technical ability to suspend an account, deny-list an address, freeze tokens or burn and reissue balances. FATF treats those capabilities as useful for compliance with lawful authority requests [4]. Legal authority must come from the competent procedure; technical control only supplies the means of execution. A China-facing request should identify the issuing authority, legal basis, token contract, address, transaction hash, amount, scope, duration and urgency, and should distinguish preservation of records from immobilisation or return of assets. Emergency action should be confirmed, reviewed and lifted when its legal basis expires.

Routine cross-border reconstruction can proceed through structured requests to the platform, issuer, custodian or home supervisor for specified onboarding, order, wallet, login and transfer records. Urgent cases may seek immediate preservation and, where legally available, narrowly defined freezing pending formal process. The revised Anti-Money Laundering Law authorises international cooperation and information exchange through competent authorities (AML Law, arts. 46--49). It also provides that, where a foreign state or organisation directly requests customer identity or transaction data, or the seizure, freezing or transfer of domestic funds or assets, in violation of the principles of reciprocity or mutual agreement, a domestic financial institution may not act on the request on its own; personal-information and data-security rules continue to govern the exchange (AML Law, art. 50).

The framework remains legally bounded only when each participant's duty is tied to its actual function, information access and lawful authority, and when the evidential threshold rises with the intrusiveness of the measure.

5. Conclusion

Dollar stablecoins preserve intermediated financial functions even when value moves through self-hosted wallets and public ledgers. A single economic transfer is divided among account institutions, exchanges, OTC converters, custodians, issuers and wallet users, leaving each participant with only part of the regulatory record. Regulatory bypass therefore arises when the account-address-account sequence no longer carries a verifiable link among the customer, fiat payment, wallet control, on-chain transfer and conversion function. This diagnosis places the regulatory focus at the fiat interface. International standards already allocate duties according to exchange, transfer, custody, issuance and customer-facing functions and require originator, beneficiary and transaction information to remain available across regulated segments. Their practical reach ends where no obliged entity participates, an offshore provider lacks an enforceable host-state connection, or an analytics inference is treated as a substitute for attribution. China's prohibition-based framework can address those gaps through interface-specific duties. Banks and payment institutions should begin enhanced scrutiny when several mutually consistent facts establish a recognisable stablecoin connection. Responsibility for commercial conversion should attach to the party that sets the rate, matches counterparties, collects fiat or releases tokens, including domestic facilitators. Records held by offshore platforms, custodians and issuers should be preserved and produced through lawful cross-border channels once targeted solicitation, domestic facilitation, recurring settlement through Chinese accounts or comparable facts establish a sufficient China-facing connection; mere technical accessibility carries little weight. The interface record should connect account data, order and pricing information, wallet-control evidence, transaction hashes and the materials explaining the correspondence between the fiat and token legs. Blockchain analytics remains useful for screening and reconstruction, provided that source, methodology, confidence, hop distance and later corrections are recorded. Legal consequences must track the evidence. A weak connection supports inquiry and monitoring; corroborated account, customer and on-chain facts can support a focused refusal, restriction or suspicious-transaction report; freezing, administrative liability and criminal referral require stronger corroboration and competent legal authority. A transaction hash identifies the recorded transfer but does not prove its controller, purpose or beneficiary. Proportionality, human review, reasoned records, correction, complaint and time-limited emergency powers keep look-through governance within the rule of law. The same limits confine data collection to the conversion under review and route cross-border disclosure through applicable personal-information, data-security and supervisory-cooperation mechanisms. Effective reconstruction does not require surveillance of every blockchain transfer. Each actor preserves the links its function can generate, and each public or private decision-maker imposes consequences only to the extent those links have been proved.

References

1. M. Reuter, *Decrypting Crypto: How to Estimate International Stablecoin Flows*, IMF Working Paper No. 2025/141, International Monetary Fund, Washington, DC, USA, 2025, doi: 10.5089/9798229016186.001.
2. Committee on Payments and Market Infrastructures (CPMI), *Considerations for the use of stablecoin arrangements in cross-border payments*, Bank for International Settlements, Basel, Switzerland, 2023.
3. T. Adrian et al., *Understanding Stablecoins*, IMF Departmental Paper No. 2025/009, International Monetary Fund, Washington, DC, USA, 2025, doi: 10.5089/9798229024075.087.
4. Financial Action Task Force (FATF), *Targeted Report on Stablecoins and Unhosted Wallets -- Peer-to-Peer Transactions*, FATF, Paris, France, 2026.
5. B. Hofmann, A. Mehrotra, and J. Paulick, *Dollarisation and monetary control: what lessons for the rise of stablecoins?*, BIS Working Papers No. 1370, Bank for International Settlements, Basel, Switzerland, 2026.
6. R. K. Lyons and G. Viswanath-Natraj, "What keeps stablecoins stable?," *Journal of International Money and Finance*, vol. 131, p. 102777, 2023, doi: 10.1016/j.jimonfin.2022.102777.
7. A. Ferreira, "The Curious Case of Stablecoins-Balancing Risks and Rewards?," *Journal of International Economic Law*, vol. 24, no. 4, pp. 755–778, 2021, doi: 10.1093/jiel/jgab036.
8. F. Cengiz, "Stablecoins and their regulation: a Hayekian approach," *Journal of International Economic Law*, vol. 28, no. 2, pp. 204–223, 2025, doi: 10.1093/jiel/jgaf014.
9. Financial Stability Board (FSB), *High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final report*, FSB, Basel, Switzerland, 2023.
10. Financial Action Task Force (FATF), *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, France, 2021.
11. International Monetary Fund and Financial Stability Board, *IMF-FSB Synthesis Paper: Policies for Crypto-Assets*, International Monetary Fund and Financial Stability Board, Washington, DC, USA and Basel, Switzerland, 2023.
12. Financial Stability Board, *Thematic Review on FSB Global Regulatory Framework for Crypto-asset Activities: Peer review report*, FSB, Basel, Switzerland, 2025.
13. Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*, updated June 2026, FATF, Paris, France, 2012–2026.
14. Financial Action Task Force (FATF), *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, France, 2025.
15. Financial Stability Board, *Cross-border Regulatory and Supervisory Issues of Global Stablecoin Arrangements in EMDEs*, FSB, Basel, Switzerland, 2024.
16. B. Gu and T. Liu, "Enforcing International Financial Regulatory Reforms," *Journal of International Economic Law*, vol. 17, no. 1, pp. 139–176, 2014, doi: 10.1093/jiel/jgu002.
17. S. L. Schwarcz, "Regulating Global Stablecoins: A Model-Law Strategy," *Vanderbilt Law Review*, vol. 75, no. 6, pp. 1729–1785, 2022.
18. M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert, and P. Pesch, "Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations," *Forensic Science International: Digital Investigation*, vol. 33, p. 200902, 2020, doi: 10.1016/j.fsidi.2019.200902.
19. L. Ye and Y. Wu, "An Outline of 'Look-Through' Regulation in Financial Markets," *Law Science*, no. 12, pp. 12–21, 2017.
20. Y. Zheng, "Application and Restriction on 'Looking-Through Regulation': Financial Instrument, Systemic Risk and Regulation Boundary," *Journal of Business Economics*, no. 4, pp. 94–104, 2024, doi: 10.14134/j.cnki.cn33-1336/f.2024.04.008.
21. P. Liu, "On Blockchain Evidence," *Chinese Journal of Law*, no. 6, pp. 130–148, 2021.
22. H. Xing, "Are Financial Regulatory Measures a New Type of Administrative Act?," *Peking University Law Journal*, vol. 26, no. 3, pp. 730–746, 2014.
23. Disclaimer/Publisher's Note: The statements, opinions and data contained in this publication are solely those of the author. The publisher and editor disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.