StoneX

StoneX Digital International Limited (SDI)

Conflicts of Interest Disclosure

(pursuant to Article 72(2) of Regulation (EU) 2023/1114 on Markets in Crypto-Assets)

Version 4.0

August 2026

STONEX DIGITAL INTERNATIONAL LTD
3rd Floor, Portview House, Thorncastle Street, Dublin 4, Ireland Company Registration No. 751872
Authorised and regulated by the Central Bank of Ireland
www.stonex.com

Managing conflicts of interest at SDI

StoneX Digital International Limited ("**SDI**") is a company incorporated in Ireland and is authorised and regulated by the Central Bank of Ireland as a crypto-asset service provider ("**CASP**") pursuant to Regulation (EU) 2023/1114 on Markets in Crypto-Assets ("**MiCAR**").

Under Article 72 of MiCAR, CASPs are required to maintain and operate effective organisational and administrative arrangements designed to identify, prevent, manage and disclose conflicts of interest that may arise in the course of providing crypto-asset services. These requirements are supplemented by Commission Delegated Regulation (EU) 2025/1142, which prescribes detailed rules concerning conflicts of interest policies, governance arrangements and public disclosures.

Article 72(1) requires CASPs to maintain policies and procedures to identify conflicts between:

- The CASP and its shareholders or members;
- The CASP and persons linked to it by control;
- The CASP and members of its management body;
- The CASP and its employees;
- The CASP and its clients; or
- Two or more clients whose interests conflict with one another

Accordingly, conflicts of interest may arise where the interests of SDI, its shareholders, directors, employees, outsourced service providers, affiliates within the StoneX Group, or other connected persons diverge from, or potentially compete with, the interests of a client. The existence of a conflict of interest does not, in itself, imply misconduct or regulatory non-compliance. Rather, conflicts of interest may arise in the ordinary course of business and do not, in themselves, indicate misconduct or regulatory non-compliance. Such conflicts must be appropriately identified, assessed, managed and controlled through effective governance and oversight arrangements.

SDI has established and maintains a comprehensive conflicts of interest framework designed to identify actual, potential and perceived conflicts of interest arising from its business activities. The framework is supported by governance arrangements proportionate to the nature, scale and complexity of SDI's operations and includes, among other measures, independent oversight, segregation of duties, information barriers, personal account dealing controls, remuneration arrangements designed to avoid inappropriate incentives, and disclosure and recusal procedures applicable to directors, senior management and employees.

All identified conflicts are assessed on a risk-sensitive basis and recorded within SDI's Conflicts of Interest Register. Appropriate preventative, mitigating or monitoring measures are applied having regard to the nature and materiality of the conflict. The operation and effectiveness of these controls are subject to ongoing oversight by the Compliance Function and periodic reporting to the Board of Directors.

This disclosure is published in accordance with Article 72 of MiCAR. Article 72(2) of MiCAR requires a CASP to disclose to its clients and prospective clients the general nature and sources of conflicts of interest and the steps taken to mitigate those conflicts where the organisational and administrative arrangements established by the CASP are not sufficient to ensure, with reasonable confidence, that risks of damage to client interests will be prevented.

In line with Article 72(2) of MiCAR, the Annex to this disclosure contains a summary of the conflicts recorded in SDI's Conflicts of Interest Register, together with the controls and mitigation measures implemented to manage those conflicts. This disclosure is reviewed periodically and updated to reflect any material changes to SDI's business activities, organisational arrangements or conflict risk profile.

Annex: Summary of SDI Conflicts of Interest Register

Area	Potential Conflict	Risk	Mitigation
Organisational Conflict: SDI & Group Entities			
Organisational Conflict: SDI & Group Entities	Intra-Group Execution	A conflict arises where SDI routes client orders to SDX, its group affiliate, for execution, so that Group revenue considerations could compete with SDI's duty to obtain the best possible result for the client.	SDI and SDX operate independent governance and separate management structures, supported by robust information barriers that prevent inappropriate data sharing. Order handling follows SDI's Order Execution Policy, which is available for review on our website and governs how client orders are handled fairly and in clients' best interests. Execution quality is subject to compliance monitoring and post-trade review, and the Central Bank of Ireland monitors SDI's use of matched principal trading under Article 72 of MiCAR.
Organisational Conflict: SDI & Group Entities or External interests (Internal)	Dual Shareholding Across SDI and External Service Providers	Conflicts of interest may occur if SDI shareholders or their affiliates have stakes in external service providers, potentially leading to biased procurement decisions or terms that do not align with client interests.	These interests must be disclosed and are reviewed through the SDI conflict disclosure process, and the individuals involved are recused from related decisions. Separately, all SDI contracts undergo rigorous independent, arm's-length assessment under our third-party management framework, the Vendor Risk Management guidelines and the Outsourcing Policy.
Organisational Conflict: SDI & Group Entities	Group Shareholder Conflicts in Strategic Decision-Making	Parties linked to SDI shareholders may hold interests in group affiliates or external service providers, which could influence decisions in favour of Group interests rather than clients.	These relationships must be disclosed and are assessed under the SDI conflict disclosure process, with governance structures, independent oversight and formal review ensuring client interests are protected at all times. Where a material conflict cannot be prevented or mitigated, it is escalated to the SDI Board for consideration.
Organisational Conflict: SDI & Group Entities	Intragroup Outsourcing and Self-Review	SDI relies on functions performed by, or shared with, other StoneX Group entities, including personal account dealing surveillance carried out by the StoneX	Each outsourced function has a named owner within SDI Compliance and is governed by intragroup service and outsourcing agreements with defined service levels. SDI

Area	Potential Conflict	Risk	Mitigation
		EMEA Central Surveillance Team and Financial Crime Prevention services. A conflict arises where the same Group entity both performs an operational function for SDI and provides the compliance or internal audit assurance over that function, creating a self-review risk across the three lines of defense.	evidences functional segregation within the provider, independently challenges the advice and findings it receives, and applies ongoing outsourcing oversight. Material intragroup conflicts are recorded in the Conflicts of Interest Register and reported to the SDI Board.
Organisational Conflict: SDI & Internal			
Organisational Conflict: SDI & Internal	Resource Allocation Between SDI and Internal Functions	This conflict arises from competing demands for shared resources such as technology, infrastructure or staff across teams, which may result in SDI activities being deprioritised.	To prevent performance issues, we use clear contracts and service level agreements to ensure accountability and align expectations. This is further supported by a robust business continuity plan that maintains service stability under internal pressure.
Organisational Conflict: SDI & Internal	Overlapping Senior Management Functions	This conflict may arise from shared directors or executives favouring one entity over another, leading to bias or misaligned priorities.	We maintain separate management teams and enforce strong information barriers to ensure independent, objective decision-making. Members of the management body and executive committees declare all roles held within the StoneX Group on appointment and as they arise thereafter, and recuse themselves from any deliberation or decision in which they have an actual or potential conflict.
Organisational Conflict: SDI & Internal	Information Sharing Between Group Entities	This conflict arises from the risk of misusing or improperly sharing confidential group-level information, potentially disadvantaging an entity or a client and causing trust or regulatory issues.	Mitigation measures include market abuse and inside information policies, robust access controls and information barriers between business lines involved in potentially conflicting activities, together with ongoing training to ensure compliance with data privacy and inside information requirements. These controls are maintained in line with Article 3 of Commission Delegated Regulation (EU) 2025/1142 and the SDI Market Conduct Policy.
Organisational Conflict: SDI & Internal	Custody and Service-Line Segregation	Providing custody and administration of crypto-assets alongside execution and other services may create incentives to use client assets or client information in a way that favours another SDI activity.	SDI functionally and hierarchically separates custody activities from other activities that may give rise to conflicts. Segregation of duties ensures that conflicting activities are not carried out by the same or connected individuals, including the separation of trade execution from settlement

Area	Potential Conflict	Risk	Mitigation
			and reconciliation, and the separation of control and oversight functions from client-facing functions.
Organisational Conflict: SDI & Internal	Matched Principal Execution and Risk Management	Because SDI interposes itself between buyer and seller, and may hedge exposure arising from client activity, its own interest in the outcome of a transaction could be perceived to compete with the client's interest in that outcome.	SDI executes on a matched principal basis, with both sides executed simultaneously so that SDI is not exposed to market risk throughout the execution. Hedging of client exposure is undertaken only as legitimate risk management and is treated as such under the Conflicts of Interest Policy. Pricing and order handling are governed by the Order Execution Policy and monitored by Compliance, and the Central Bank of Ireland monitors SDI's use of matched principal trading pursuant to Article 72 of MiCAR.
Organisational Conflict: SDI & Internal	Remuneration-Linked Incentives	Remuneration linked to the revenue of a particular activity could incentivise staff, outsourced personnel or members of the management body to favour that activity over the interests of clients.	SDI removes direct links between remuneration and the revenues generated by activities that may conflict, in line with Article 5 of Commission Delegated Regulation (EU) 2025/1142 and the Group Remuneration Policy. Remuneration is not predominantly based on quantitative commercial criteria, and performance reviews take into account compliance metrics, fair treatment of clients and service-quality metrics. Individuals with remuneration incentives for one activity do not hold decision-making authority or exercise inappropriate influence over conflicting activities.
External: SDI and competitor CASP			
External: SDI and competitor CASP	Management Body Member with Interest in a Competing CASP	A Board member with interests in a competing crypto-asset service provider may encounter divided fiduciary duties or risk the disclosure of sensitive strategic information, thereby compromising governance and client protection.	Members of the management body are prohibited from holding positions in other crypto-asset businesses outside the StoneX Group. All external interests must be fully disclosed at the point of appointment and as they arise, with mandatory recusals and restrictions enforced in accordance with Board protocols and subject to compliance oversight, including periodic screening for external directorships and non-Group roles. Directors' duties under sections 228 and 231 of the Companies Act

Area	Potential Conflict	Risk	Mitigation
			2014 apply, and all declared interests are recorded in the Conflicts of Interest Register.
SDI Employees			
SDI Employees	Client Order Prioritisation Conflict	Conflicts may occur when multiple clients place orders for the same crypto-asset in illiquid markets, creating a risk of preferential execution that could undermine fairness and client trust.	SDI enforces its Order Execution Policy, published on the firm's website, to ensure consistent treatment of all orders. The policy applies objective criteria and subjects execution to compliance monitoring and post-trade review.
SDI Employees	Employee Personal Interest in Client Business	A conflict may arise if an SDI employee holds a directorship or financial interest in a client, creating the potential for bias in decisions related to transactions, referrals or onboarding.	All external roles require prior approval under the Outside Business Activities requirements of the SDI Conflicts of Interest Policy and StoneX's outside business interests policy, with controls such as role restrictions, recusal and regular conflict reviews in place. Staff declare outside interests on appointment and attest annually.
SDI Employees	Insider Knowledge and Personal Trading Conflict	A conflict may arise if an employee holds crypto-assets in a project listed by SDI while having access to confidential information, risking misuse or the appearance of insider trading. This can harm client trust and expose SDI to regulatory action.	The SDX/SDI Personal Account Dealing Policy requires pre-clearance of trades in crypto-assets and other specified assets, assessed against identified conflicts by the StoneX EMEA Central Surveillance Team, together with declaration of all personal dealing accounts and annual attestation. Enhanced monitoring applies to employees with access to sensitive information, and breaches are reported to the Head of SDI Compliance. All actual and potential conflicts are reviewed by Compliance and recorded in the Conflicts Register. SDI also enforces market abuse and inside information policies, supported by strict access controls and ongoing training.
SDI Employees	Client Inducement and Preferential Treatment Risk	A conflict can happen if a client gives gifts or incentives to SDI staff to secure special treatment. This could lead to unfair treatment of other clients and damage trust.	SDI enforces a strict Anti-Bribery and Corruption Policy, Code of Conduct and Gifts & Entertainment policies, supported by annual training, mandatory reporting, compliance oversight and disciplinary measures. Material or recurring gifts and hospitality that may create a conflict must also be disclosed to Compliance.

Area	Potential Conflict	Risk	Mitigation
SDI Employees	Employee Holding Client Directorship Risk	An employee serving as a director of a client may create a conflict between their duties to SDI and to the client, creating the potential for bias in decision-making or blurred boundaries.	Such roles must be declared and reviewed under the Outside Business Activities requirements, with controls such as role separation, recusal and regular monitoring to maintain objectivity.
SDI Employees	Employee Trading in Client-Issued Crypto-Assets	Employee trading in crypto-assets transacted by clients may raise risks of insider dealing or confidentiality breaches, harming market integrity and client trust.	SDI mitigates this through its Personal Account Dealing and Market Conduct policies, requiring pre-clearance and disclosure of holdings as well as annual training. Breaches are subject to disciplinary action.
SDI Employees	Family Relationships and Related Parties	Close personal or family relationships within a reporting line, business conducted on SDI's behalf with a connected person, or recruitment involving a related candidate may compromise objective decision-making.	No employee may sit within a managerial reporting line, at any degree of separation, of a person to whom they are closely related; any such situation must be escalated to HR and SDI Compliance before an offer is made. Business with connected persons requires prior written approval from senior management, and significant engagements are considered by the SDI Risk Committee. Interviewers with a familial or financial relationship to a candidate stand down from the process and are not eligible for a referral bonus.
SDI Employees	Vendor Selection and Procurement	An employee with a personal interest in a vendor or prospective vendor could influence a tender or contract award away from the best interests of SDI and its clients.	No employee may accept any benefit of any kind in return for the promise of a vendor contract, including in a competitive tender. Vendor selection follows the Vendor Risk Management guidelines and the Outsourcing Policy, and any staff member with a personal interest in a vendor or potential vendor is recused from all related decision-making.
SDI Employees	Third-Party Inducements and Loans	Fees, commissions or other benefits received from a person other than the client in relation to a service provided to that client, or lending arrangements between staff and clients or vendors, could distort how clients are treated.	SDI will not accept or retain any fees, commissions or monetary or non-monetary benefits provided by a third party in relation to services to clients; only minor benefits such as seminars, conferences and de minimis hospitality may be accepted. Employees may not make or receive loans to or from clients, vendors, regulators or other contractual or prospective counterparties of SDI, other than in the context

Area	Potential Conflict	Risk	Mitigation
			of long-term banking relationships with commercial organisations.