

StoneX Digital International Limited (SDI)

Conflicts of Interest Register

Version 3.0

November 2025

SDI Conflict Risks and Mitigations Disclosure

Area	Potential Conflict	Risk	Conflict of Interest 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	This conflict is mitigated to ensure SDI maintains its obligation to secure fair client execution. To manage these risks, SDI and SDX operate with independent governance and separate management structures, supported by robust information barriers to prevent inappropriate data sharing. SDI adheres to a transparent Order Execution Policy that governs how client orders are handled fairly and in clients' best interests—this policy is available for review on our website.
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. Individuals involved are recused from related decisions. Separate to this process all contracts for SDI, undergo rigorous independent, arm's-length assessment as part of our third-party Management framework.
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 favor of group interests rather than clients.	These relationships must be disclosed. They will be assessed under the SDI conflict disclosure process, with governance structures, independent oversight, and formal review ensuring client interests are protected at all times.
Organisational Conflict: SDI & Internal			
Organisational Conflict: SDI & Internal	Resource Allocation Conflict - Between SDI and Internal	This conflict arises from competing demands for shared resources like technology, infrastructure, or staff across teams.	To prevent performance issues, we use clear contracts and SLAs to ensure accountability and align expectations. This is further supported by a robust business continuity plan for service stability under internal pressure
Organisational Conflict: SDI & Internal	Overlapping Senior management functions	This conflict may arise from shared directors or executives favoring one entity over another, leading to bias or misaligned priorities.	We mitigate this by maintaining separate management teams and enforcing strong information barriers to ensure independent, objective decision-making.
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 and causing trust or regulatory issues.	Mitigation measures include the implementation of market abuse and insider information related policies as well as robust access controls, and ongoing training to ensure compliance with data privacy and insider information regulation
External: SDI and competitor Firms	Management Body Member with Interest in a Competing CASP	An SDX Board member with interests in a competing Crypto-Asset Service Provider (CASP) may encounter divided fiduciary duties or risk the disclosure of sensitive strategic information, thereby compromising governance and client protection	All external interests must be fully disclosed, with mandatory recusals and restrictions enforced in accordance with Board protocols and subject to compliance oversight.

Area	Potential Conflict	Risk	Conflict of Interest Mitigation
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.
	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 StoneX's Outside Business Interests Policy, with controls such as role restrictions, recusal, and regular conflict reviews in place.
	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 Transaction Policy mandates pre-approval and disclosure of holdings, with enhanced monitoring for employees who have access to sensitive information. All actual and potential conflicts are reviewed by Compliance and recorded in the Conflicts Register. In addition, SDI enforces market abuse and insider information policies, supported by strict access controls and ongoing training to ensure adherence to applicable regulations.
	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 and damage trust.	SDI enforces a strict Anti-Bribery and Corruption Policy, Code of conduct and Gifts & Entertainments policies, supported by annual training, mandatory reporting, compliance oversight, and disciplinary measures.
	Employee Holding Client Directorship Risk	An employee serving as a director of a client may create a conflict between their duties to SDI and the client, creating the potential for bias in decision making or blurred boundaries.	Such roles must be declared and reviewed under Outside Work Policies, with controls like role separation, recusal, and regular monitoring to maintain objectivity.
	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 Transaction and Market Abuse Policies, requiring pre-approval and disclosure of holdings as well as annual training. Breaches are subject to disciplinary action.