Your Business Requirements

Asset Management

AM Public

- A significant portion of AM Public's money laundering risk relates to third-party intermediaries (e.g., third-party distributors and sub-transfer agents). If these intermediaries have deficient controls, illicit proceeds may be introduced into AM Public's funds and/or managed through AM Public's separate account, wrap fee or other advisory programs.
- Customers who invest directly may similarly introduce tainted, corrupt, or illicit proceeds into the AM Public funds.
- Lack of transparency to underlying investors of accounts intermediated by third-party distributors.
- Inadequate due diligence on external hedge funds and private equity managers selected through the External Investment Group (XIG) platform may expose fund investors to potential securities fraud or potential undetected risks at portfolio companies.

AM Private

- AM Private's primary risk involves potential undetected risks at portfolio companies (e.g., those introduced by subsidiaries/affiliates) and/or portfolio companies that operate in high-risk jurisdictions, high-risk industries, and/or that fail to maintain effective controls to mitigate the risk of bribery and government sanctions violations.
- AM Private investors may also pose money laundering risk (e.g., touchpoints to high-risk jurisdictions or politically exposed persons). While these investors have generally been customers of other areas of the firm, the current focus on sales through third-party intermediaries and direct to institutional clients increases the risk that illicit proceeds may be introduced into AM Private's sales and/or managed through AM Private's separate accounts.
- Enhanced due diligence, ongoing assessment of portfolio company risks, and escalation of issues are key elements of mitigating these money laundering and reputational risks.

Due diligence, ensuring the adequacy of legal covenants and Service-Level Agreements, and timely escalation of issues are critical elements of mitigating these money laundering and reputational risks.

Consumer

- Risk of tainted assets (e.g., proceeds of corruption, illegal funds) being deposited into the bank or indirectly deposited due to AML failures at omnibus deposit brokers

- Increased risk for identity theft, synthetic identity, and large fraud rings for online platform

Red Flags

Examples of typical red flags for suspicious activity in the Consumer business include customers who:

- Have transaction activity move through the account in a rapid manner

- Have funds transfer activity to or from secrecy havens (e.g., Cayman Islands) or higher risk locations without apparent purpose

- Repeatedly overpay a loan or balance, and then follow with requests to refund the funds

- Have repeated round-dollar purchase amounts with the same merchant in a short period of time

- Payoff loans early outside of what is known about the customer's financial wealth

- Attempt to make cash payments toward a loan balance

- Attempt to make cash payments toward a loan balance

- Attempt to make frequent or large deposits of currency, insist on dealing only in cash equivalents, or ask for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

- Purchase a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold.

- Have frequent and unusual use of the card for withdrawing cash at ATMs.

- Have large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.

- Have unusual cash advance activity and large cash payments: the monitoring of incoming cash is critical as excessive cash payments are often an attribute of money laundering. Credit balance accumulation resulting in refunds (CBRs) should be monitored as they can be used as part of a scheme to launder funds.

- Attempt multiple and frequent cash payment or money orders; large, cross-border wire transfer payments.

GBM Public

- Primary money laundering risks in GBM Public include insider trading and various forms of market manipulation/abuse (e.g., microcap fraud, wash trades, marking the close, price fixing/collusion, etc.).

- Investment advisor fraud (e.g., misappropriation, Ponzi schemes) is also a significant risk for the GBM Public Prime Services businesses (PB, Prime Clearing, GSAS) as the customer base consists predominantly of third-party managers who are responsible for the investment decisions and assets of the funds they manage.

- Identify theft (e.g., fraudulent transactions) and money laundering may occur in the Prime Services businesses (PB, Prime Clearing, GSAS) due to the custodial nature of certain accounts and the frequent movement of funds.

- Internal fraud may occur in any area of GBM Public (e.g., mis-marking of firm positions, leaking of sensitive information).

- Comprehensive customer identification practices regarding fund managers, recognition of suspicious activity, and ongoing monitoring of accounts are essential to mitigating the risks in GBM Public.

Red Flags

Examples of typical red flags for suspicious activity in the GBM Public business include:

- Transaction patterns are significantly different from customer's peer group

- Funds transfers are sent or received from the same person to or from different accounts

- Customer's transactional activity moves through the account in a rapid manner with little or no intervening investment activity

- Funds transfer activity to or from secrecy havens or higher risk geographic locations without apparent purpose

- Trading activity that appears unusually timely/economically beneficial in relation to a market-moving event

- Contact from new email addresses/phone numbers related to urgent money movement requests

Goldman Sachs

Global Investment Research (GIR)

- The principal money laundering risk with GIR is related to the receipt of MNPI and price-sensitive information.

- Research analysts may be exposed, on occasions, to confidential or proprietary information such as, corporate customer deal information (via wall crossings requested by individuals in Investment Banking) and firm proprietary information (positions, trade strategies). This information could lend itself to insider trading.

- Additionally, in the course of normal research due diligence, individuals in GIR may inadvertently obtain or receive sensitive, confidential or proprietary information from corporates, government officials, or other market participants. The relevant risks are the potential leakage of sensitive information and possible insider trading.

Investment Banking

- Investment Banking personnel regularly receive and handle confidential information, including MNPI.

- Significant risk exists related to safeguarding MNPI and maintaining information barriers.

- The receipt of MNPI could lend itself to insider trading or market manipulation.

- With respect to corruption issues, Investment Banking may provide financing or advisory services to government entities, such as central banks, ministries of finance, and sovereign wealth funds or related entities, located in jurisdictions with a heightened risk for corruption. In such instances, the nature and intended use of the financing proceeds are critical considerations in mitigating risk.

- The involvement of a high-risk or undisclosed intermediary between the customer and a government official or agency could be a red flag for bribery or corruption.

- Customers may have a business model or revenue streams with potential money laundering concerns and/or risk of tainted assets. Understanding the risk profile of the customer base or parties in the transaction/project is critical in mitigating reputational and legal impacts to the firm.

Goldman Sachs

Wealth Management (WM)

- Customer selection and due diligence are critical to ensuring risks are mitigated and that the firm understands the customer and their source of wealth. This is particularly important for WM customers with a touchpoint in – or source of wealth relating to – high-risk industries or jurisdictions.

- Wealth Management's customer base, which includes customers with political exposure, a limited number of bearer share entities, and some customers with opaque or complex ownership, presents elevated risk of money laundering, tax evasion, and/or handing or holding the proceeds of corruption or fraud.

- The frequent movement of funds into/out of WM customer accounts, including movements involving third parties, poses a heightened risk of money laundering, tax evasion, and identity theft.

- WM customers may also engage in market manipulation (including microcap fraud) and insider trading (leveraging insider information, for example).

- Recognition of suspicious activity and ongoing monitoring of accounts are also essential to mitigating risks in WM.

Red Flags

Examples of typical red flags for suspicious activity in the WM business include:

- Transaction patterns are significantly different from customer's peer group

- Funds transfers are sent or received to or from unrelated accounts

- Unusual trading in advance of a public announcement

- Funds transfer activity to or from secrecy havens or higher risk geographic locations without apparent purpose

Goldman Sachs

Transaction Banking (TxB)

- Given the international and third-party nature of products and services offered, TxB poses incremental risks from a money laundering and sanctions perspective.

- TxB's Global Payments offering presents increased money laundering and sanctions risk due to the provision of international, cross-currency, third-party funds transfer capabilities. Products that can transfer assets across borders pose a higher risk for sanctions violations and money-laundering than purely domestic products, and third-party payments introduce counterparty risk in addition to the risk potentially inherent to the customer.

- TxB's correspondent banking relationships are also particularly vulnerable to money laundering, terrorist financing and sanctions evasion because they involve carrying out transactions on behalf of the intermediary's underlying customers. TxB does not perform KYC on these underlying customers, yet is responsible for preventing and detecting any criminal activity undertaken by them via TxB.

- Commercial banking, and in particular correspondent banking, has been the focus of many of the most aggressive enforcement actions and penalties in history.