



The Wolfsberg Group Anti-Money Laundering Questionnaire

**the
Wolfsberg
Group**

Financial Institution Name	HSBC Group
Location	8 Canada Square, London E14 5HQ

The Wolfsberg Group consists of the following leading international financial institutions: Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale, Standard Chartered and UBS which aim to develop frameworks and guidance for the management of financial crime risks particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

This questionnaire acts as an aid to firms conducting due diligence and should not be relied on exclusively or excessively. Firms may use this questionnaire alongside their own policies and procedures in order to provide a basis for conducting client due diligence in a manner consistent with the risk profile presented by the client. The responsibility for ensuring adequate due diligence, which may include independent verification or follow up of the answers and documents provided, remains the responsibility of the firm using this questionnaire.

1. General AML Policies, Practices and Procedures

If you answer “No” to any question, additional information can be supplied at the end of the questionnaire.

	Yes	No
1. Is the AML compliance program approved by the FI's board or a senior committee?	Yes	
2. Does the FI have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML framework?	Yes	
3. Has the FI developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions?	Yes	
4. In addition to inspections by the government supervisors/regulators, does the FI client have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?	Yes	
5. Does the FI have a policy prohibiting accounts/relationships with shell banks? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group)	Yes	
6. Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	Yes	
7. Does the FI have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates?	Yes	
8. Does the FI have record retention procedures that comply with applicable law?	Yes	
9. Are the FI's AML policies and practices being applied to all branches and subsidiaries of the FI both in the home country and in locations outside of that jurisdiction?	Yes	

2. Risk Assessment

	Yes	No
10. Does the FI have a risk-based assessment of its customer base and their transactions?	Yes	
11. Does the FI determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?	Yes	

3. Know Your Customer, Due Diligence and Enhanced Due Diligence

	Yes	No
12. Has the FI implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?	Yes	
13. Does the FI have a requirement to collect information regarding its customers' business activities?	Yes	
14. Does the FI assess its FI customers' AML policies or practices?	Yes	
15. Does the FI have a process to review and, where appropriate, update customer information relating to high risk client information?	Yes	
16. Does the FI have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?	Yes	
17. Does the FI complete a risk-based assessment to understand the normal and expected transactions of its customers?	Yes	

4. Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds

		Yes	No
18.	Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	Yes	
19.	Where cash transaction reporting is mandatory, does the FI have procedures to identify transactions structured to avoid such obligations?	Yes	
20.	Does the FI screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities?	Yes	
21.	Does the FI have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?	Yes	
22.	Does the FI adhere to the Wolfsberg Transparency Principles and the appropriate usage of the SWIFT MT 202/202COV and MT 205/205COV message formats? ¹	Yes	

5. Transaction Monitoring

		Yes	No
23.	Does the FI have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as traveler's checks, money orders, etc?	Yes	

¹ The four payment message standards to be observed are: i) FIs should not omit, delete, or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other FI in the payment process; ii) FIs should not use any particular payment message for the purpose of avoiding detection of information by any other FI in the payment process; iii) Subject to applicable laws, FIs should cooperate as fully as practicable with other FIs in the payment process when requesting to provide information about the parties involved; and (iv) FIs should strongly encourage their correspondent banks to observe these principles.

Source: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/13.%20Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_%282007%29.pdf

6. AML Training

		Yes	No
24.	<p>Does the FI provide AML training to relevant employees that includes:</p> <ul style="list-style-type: none"> ◆ Identification and reporting of transactions that must be reported to government authorities ◆ Examples of different forms of money laundering involving the FI's products and services ◆ Internal policies to prevent money laundering 	Yes	
25.	Does the FI retain records of its training sessions including attendance records and relevant training materials used?	Yes	
26.	Does the FI communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?	Yes	
27.	Does the FI employ third parties to carry out some of the functions of the FI?	Yes	
28.	<p>If the answer to question 27 is yes, does the FI provide AML training to relevant third parties that includes:</p> <ul style="list-style-type: none"> ◆ Identification and reporting of transactions that must be reported to government authorities ◆ Examples of different forms of money laundering involving the FI's products and services ◆ Internal policies to prevent money laundering 	Yes	

Space for additional information

(Please indicate which question the information is referring to)

Question 9 – refers to all wholly owned or controlled HSBC Group of companies

Also, please note, in December 2012, HSBC entered into agreements with the US and UK authorities in relation to investigations regarding HSBC's past inadequate compliance with Anti-Money Laundering ("AML") and Sanctions laws. These agreements include the five-year Deferred Prosecution Agreement ("DPA") with the US Department of Justice, a Direction (the "Direction") issued by the UK Financial Conduct Authority ("FCA") (formerly the Financial Services Authority), and a Cease and Desist Order (the "Order") issued by the US Federal Reserve Board.

Under these agreements, Mike Cherkasky was appointed as an independent corporate compliance monitor ("the Monitor") to evaluate HSBC's progress in fully implementing our obligations and produce regular assessments of the effectiveness of HSBC's AML and Sanctions controls. The Monitor also served as a Skilled Person under the Direction and an Independent Consultant under the Order. In December 2017, at the conclusion of the five-year period, it was determined that HSBC had met its obligations under the DPA and, as a result, the DPA expired. Mike Cherkasky will continue to serve as a Skilled Person and Independent Consultant, pursuant to the respective agreements, for a period of time at the discretion of those regulators.

The issues identified in the DPA, Direction, and Order were primarily around past failures to suitably manage AML and Sanctions risk. HSBC has dramatically strengthened its ability to manage financial crime risk since 2012. This has been achieved through the combination of extensive de-risking of its customer base, tactical measures taken to mitigate interim risk and the roll out of strategic reforms. We have completed the introduction of the major compliance IT systems, put in place our AML and sanctions policy framework, and assessed our

current financial crime risk management capabilities to identify any gaps and enable integration into our day-to-day operations. All of the actions that we committed to in 2013 as part of the Global Standards programme have been completed or superseded. Further improvements are underway to make our reforms more effective and sustainable.

HSBC's Global AML Programme's ("AML Programme") objective is to ensure that money laundering risks identified by HSBC are appropriately mitigated. This is achieved by establishing: Board-approved, minimum governing policies, principles, and standards; and implementing appropriate controls, to protect HSBC, its employees, shareholders, and customers from money laundering activity. The AML Programme provides guidance to all HSBC employees, requiring them to conduct business in accordance with applicable AML laws, rules, and regulations.

The AML Programme is based upon various laws, regulations and regulatory guidance from the United Kingdom, the European Union, Hong Kong, the United States of America, and, as applicable, local jurisdictions in which HSBC does business.

The Programme includes, but is not limited to:

- ◆ The appointment of a Global and Country Money Laundering Reporting Officer ("MLRO") or alternative position as required by local regulation
- ◆ A Customer Due Diligence ("CDD") Programme, which incorporates Customer Identification and Verification ("ID&V") and Know Your Customer ("KYC") principles, and the implementing of programmes designed to appropriately remediate CDD of our existing customers
- ◆ Conducting enhanced due diligence ("EDD") on customers assessed as higher risk, such as Politically Exposed Persons ("PEPs") in senior positions, their relatives and close associates
- ◆ Establishing processes and systems designed to monitor customer transactions for the purpose of identifying suspicious activity
- ◆ The investigation and subsequent reporting of suspicious activity to the appropriate regulatory bodies
- ◆ Mandated regular independent testing and regular AML training of its employees and contractors
- ◆ The prohibition of the following products, services and customer types:
 - Anonymous accounts or numbered accounts or customers seeking to maintain an account in an obviously fictitious name
 - Shell banks, ie banks with no physical presence or staff
 - Hold Mail, ie where the customer has instructed all documentation related to the account are to be held on their behalf until collection;
 - Payable-through-accounts. HSBC does not allow domestic or foreign bank customers to provide payable-through-accounts to their customers on their HSBC accounts, and
- ◆ Any relevant additional local requirements

HSBC remains firmly committed to implementing globally consistent and rigorous financial crime controls that will help to promote the integrity of the global financial system.

Name	Ralph Nash
-------------	------------

Title	GLOBAL HEAD OF FINANCIAL CRIME COMPLIANCE and GROUP MLRO
--------------	--

Signature	
------------------	---

Date	25 May, 2018
-------------	--------------
