



Financial Institution Name: \_\_\_\_\_

Location (Country) : \_\_\_\_\_

--

No #	Question	Answer
<b>1. ENTITY &amp; OWNERSHIP</b>		
1	Full Legal Name	
2	Append a list of foreign branches which are covered by this questionnaire	
3	Full Legal (Registered) Address	
4	Full Primary Business Address (if different from above)	
5	Date of Entity incorporation/establishment	
6	Select type of ownership and append an ownership chart if available	
6 a	Publicly Traded (25% of shares publicly traded)	
6 a1	If Y, indicate the exchange traded on and ticker symbol	
6 b	Member Owned/Mutual	
6 c	Government or State Owned by 25% or more	
6 d	Privately Owned	
6 d1	If Y, provide details of shareholders or ultimate beneficial owners with a holding of 10% or more	
7	% of the Entity's total shares composed of bearer shares	
8	Does the Entity, or any of its branches, operate under an Offshore Banking License (OBL)?	
8 a	If Y, provide the name of the relevant branch/es which operate under an OBL	
9	Does the Bank have a Virtual Bank License or provide services only through online channels?	
10	Name of primary financial regulator/supervisory authority	
11	Provide Legal Entity Identifier (LEI) if available	
12	Provide the full legal name of the ultimate parent (if different from the Entity completing the DDQ)	

13	Jurisdiction of licensing authority and regulator of ultimate parent	
14	Select the business areas applicable to the Entity	
14 a	Retail Banking	
14 b	Private Banking	
14 c	Commercial Banking	
14 d	Transactional Banking	
14 e	Investment Banking	
14 f	Financial Markets Trading	
14 g	Securities Services/Custody	
14 h	Broker/Dealer	
14 i	Multilateral Development Bank	
14 j	Wealth Management	
14 k	Other (please explain)	
15	Does the Entity have a significant (10% or more) portfolio of non-resident customers or does it derive more than 10% of its revenue from non-resident customers? (Non-resident means customers primarily resident in a different jurisdiction to the location where bank services are provided)	
15 a	If Y, provide the top five countries where the non-resident customers are located.	
16	Select the closest value:	
16 a	Number of employees	
16 b	Total Assets	
17	Confirm that all responses provided in the above Section are representative of all the LE's branches.	
17 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
18	If appropriate, provide any additional information/context to the answers in this section.	
<b>2. PRODUCTS &amp; SERVICES</b>		
19	Does the Entity offer the following products and services:	
19 a	Correspondent Banking	
19 a1	If Y	
19 a1a	Does the Entity offer Correspondent Banking services to domestic banks?	
19 a1b	Does the Entity allow domestic bank clients to provide downstream relationships?	
19 a1c	Does the Entity have processes and procedures in place to identify downstream relationships with domestic banks?	
19 a1d	Does the Entity offer Correspondent Banking services to foreign banks?	
19 a1e	Does the Entity allow downstream relationships with foreign banks?	
19 a1f	Does the Entity have processes and procedures in place to identify downstream relationships with foreign banks?	
19 a1g	Does the Entity offer Correspondent Banking services to regulated Money Services Businesses (MSBs)/Money Value Transfer Services (MVTs)?	
19 a1h	Does the Entity allow downstream relationships with MSBs, MVTs, or Payment Service Provider (PSPs)?	
19 a1h1	MSBs	
19 a1h2	MVTs	
19 a1h3	PSPs	

19 a1i	Does the Entity have processes and procedures in place to identify downstream relationships with MSBs /MVTs/PSPs?	
19 b	Cross-Border Bulk Cash Delivery	
19 c	Cross-Border Remittances	
19 d	Domestic Bulk Cash Delivery	
19 e	Hold Mail	
19 f	International Cash Letter	
19 g	Low Price Securities	
19 h	Payable Through Accounts	
19 i	Payment services to non-bank entities who may then offer third party payment services to their customers?	
19 i1	If Y , please select all that apply below?	
19 i2	Third Party Payment Service Providers	
19 i3	Virtual Asset Service Providers (VASPs)	
19 i4	eCommerce Platforms	
19 i5	Other - Please explain	
19 j	Private Banking	
19 k	Remote Deposit Capture (RDC)	
19 l	Sponsoring Private ATMs	
19 m	Stored Value Instruments	
19 n	Trade Finance	
19 o	Virtual Assets	
19 p	For each of the following please state whether you offer the service to walk-in customers and if so, the applicable level of due diligence:	
19 p1	Check cashing service	
19 p1a	If yes, state the applicable level of due diligence	
19 p2	Wire transfers	
19 p2a	If yes, state the applicable level of due diligence	
19 p3	Foreign currency conversion	
19 p3a	If yes, state the applicable level of due diligence	
19 p4	Sale of Monetary Instruments	
19 p4a	If yes, state the applicable level of due diligence	
19 p5	If you offer other services to walk-in customers please provide more detail here, including describing the level of due diligence.	
19 q	Other high-risk products and services identified by the Entity (please specify)	
20	Confirm that all responses provided in the above Section are representative of all the LE's branches.	
20 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
21	If appropriate, provide any additional information/context to the answers in this section.	
<b>3. AML, CTF &amp; SANCTIONS PROGRAMME</b>		
22	Does the Entity have a programme that sets minimum AML, CTF and Sanctions standards regarding the following components:	
22 a	Appointed Officer with sufficient experience/expertise	
22 b	Adverse Information Screening	
22 c	Beneficial Ownership	
22 d	Cash Reporting	
22 e	CDD	
22 f	EDD	
22 g	Independent Testing	
22 h	Periodic Review	
22 i	Policies and Procedures	
22 j	PEP Screening	
22 k	Risk Assessment	
22 l	Sanctions	

22 m	Suspicious Activity Reporting	
22 n	Training and Education	
22 o	Transaction Monitoring	
23	How many full time employees are in the Entity's AML, CTF & Sanctions Compliance Department?	
24	Is the Entity's AML, CTF & Sanctions policy approved at least annually by the Board or equivalent Senior Management Committee? If N, describe your practice in Question 29.	
25	Does the Board receive, assess, and challenge regular reporting on the status of the AML, CTF, & Sanctions programme?	
26	Does the Entity use third parties to carry out any components of its AML, CTF & Sanctions programme?	
26 a	If Y, provide further details	
27	Does the entity have a whistleblower policy?	
28	Confirm that all responses provided in the above Section are representative of all the LE's branches	
28 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
29	If appropriate, provide any additional information/context to the answers in this section.	
<b>4. ANTI BRIBERY &amp; CORRUPTION</b>		
30	Has the Entity documented policies and procedures consistent with applicable ABC regulations and requirements to reasonably prevent, detect and report bribery and corruption?	
31	Does the Entity have an enterprise wide programme that sets minimum ABC standards?	
32	Has the Entity appointed a designated officer or officers with sufficient experience/expertise responsible for coordinating the ABC programme?	
33	Does the Entity have adequate staff with appropriate levels of experience/expertise to implement the ABC programme?	
34	Is the Entity's ABC programme applicable to:	
35	Does the Entity have a global ABC policy that:	
35 a	Prohibits the giving and receiving of bribes? This includes promising, offering, giving, solicitation or receiving of anything of value, directly or indirectly, if improperly intended to influence action or obtain an advantage.	
35 b	Includes enhanced requirements regarding interaction with public officials?	
35 c	Includes a prohibition against the falsification of books and records (this may be within the ABC policy or any other policy applicable to the Legal Entity)?	
36	Does the Entity have controls in place to monitor the effectiveness of their ABC programme?	
37	Does the Board receive, assess, and challenge regular reporting on the status of the ABC programme?	
38	Has the Entity's ABC Enterprise Wide Risk Assessment (EWRA) been completed in the last 12 months?	
38 a	If N, provide the date when the last ABC EWRA was completed.	
39	Does the Entity have an ABC residual risk rating that is the net result of the controls effectiveness and the inherent risk assessment?	
40	Does the Entity's ABC EWRA cover the inherent risk components detailed below:	
40 a	Potential liability created by intermediaries and other third-party providers as appropriate	

40 b	Corruption risks associated with the countries and industries in which the Entity does business, directly or through intermediaries	
40 c	Transactions, products or services, including those that involve state-owned or state-controlled entities or public officials	
40 d	Corruption risks associated with gifts and hospitality, hiring/internships, charitable donations and political contributions	
40 e	Changes in business activities that may materially increase the Entity's corruption risk	
41	Does the Entity's internal audit function or other independent third party cover ABC Policies and Procedures?	
42	Does the Entity provide mandatory ABC training to:	
42 a	Board and senior Committee Management	
42 b	1st Line of Defence	
42 c	2nd Line of Defence	
42 d	3rd Line of Defence	
42 e	Third parties to which specific compliance activities subject to ABC risk have been outsourced	
42 f	Non-employed workers as appropriate (contractors/consultants)	
43	Does the Entity provide ABC training that is targeted to specific roles, responsibilities and activities?	
44	Confirm that all responses provided in the above Section are representative of all the LE's branches	
44 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
45	If appropriate, provide any additional information/context to the answers in this section.	
<b>5. AML, CTF &amp; SANCTIONS POLICIES &amp; PROCEDURES</b>		
46	Has the Entity documented policies and procedures consistent with applicable AML, CTF & Sanctions regulations and requirements to reasonably prevent, detect and report:	
46 a	Money laundering	
46 b	Terrorist financing	
46 c	Sanctions violations	
47	Are the Entity's policies and procedures updated at least annually?	
48	Has the Entity chosen to compare its policies and procedures against:	
48 a	U.S. Standards	
48 a1	If Y, does the Entity retain a record of the results?	
48 b	EU Standards	
48 b1	If Y, does the Entity retain a record of the results?	
49	Does the Entity have policies and procedures that:	
49 a	Prohibit the opening and keeping of anonymous and fictitious named accounts	
49 b	Prohibit the opening and keeping of accounts for unlicensed banks and/or NBFIs	
49 c	Prohibit dealing with other entities that provide banking services to unlicensed banks	
49 d	Prohibit accounts/relationships with shell banks	
49 e	Prohibit dealing with another entity that provides services to shell banks	
49 f	Prohibit opening and keeping of accounts for Section 311 designated entities	
49 g	Prohibit opening and keeping of accounts for any of unlicensed/unregulated remittance agents, exchanges houses, casa de cambio, bureaux de change or money transfer agents	
49 h	Assess the risks of relationships with domestic and foreign PEPs, including their family and close associates	

49 i	Define the process for escalating financial crime risk issues/potentially suspicious activity identified by employees	
49 j	Define the process, where appropriate, for terminating existing customer relationships due to financial crime risk	
49 k	Define the process for exiting clients for financial crime reasons that applies across the entity, including foreign branches and affiliates	
49 l	Define the process and controls to identify and handle customers that were previously exited for financial crime reasons if they seek to re-establish a relationship	
49 m	Outline the processes regarding screening for sanctions, PEPs and Adverse Media/Negative News	
49 n	Outline the processes for the maintenance of internal "watchlists"	
50	Has the Entity defined a risk tolerance statement or similar document which defines a risk boundary around their business?	
51	Does the Entity have record retention procedures that comply with applicable laws?	
51 a	If Y, what is the retention period?	
52	Confirm that all responses provided in the above Section are representative of all the LE's branches	
52 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
53	If appropriate, provide any additional information/context to the answers in this section.	
<b>6. AML, CTF &amp; SANCTIONS RISK ASSESSMENT</b>		
54	Does the Entity's AML & CTF EWRA cover the inherent risk components detailed below:	
54 a	Client	
54 b	Product	
54 c	Channel	
54 d	Geography	
55	Does the Entity's AML & CTF EWRA cover the controls effectiveness components detailed below:	
55 a	Transaction Monitoring	
55 b	Customer Due Diligence	
55 c	PEP Identification	
55 d	Transaction Screening	
55 e	Name Screening against Adverse Media/Negative News	
55 f	Training and Education	
55 g	Governance	
55 h	Management Information	
56	Has the Entity's AML & CTF EWRA been completed in the last 12 months?	
56 a	If N, provide the date when the last AML & CTF EWRA was completed.	
57	Does the Entity's Sanctions EWRA cover the inherent risk components detailed below:	
57 a	Client	
57 b	Product	
57 c	Channel	
57 d	Geography	
58	Does the Entity's Sanctions EWRA cover the controls effectiveness components detailed below:	
58 a	Customer Due Diligence	
58 b	Governance	
58 c	List Management	
58 d	Management Information	

58 e	Name Screening	
58 f	Transaction Screening	
58 g	Training and Education	
59	Has the Entity's Sanctions EWRA been completed in the last 12 months?	
59 a	If N, provide the date when the last Sanctions EWRA was completed.	
60	Confirm that all responses provided in the above Section are representative of all the LE's branches	
60 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
61	If appropriate, provide any additional information/context to the answers in this section.	
<b>7. KYC, CDD and EDD</b>		
62	Does the Entity verify the identity of the customer?	
63	Do the Entity's policies and procedures set out when CDD must be completed, e.g. at the time of onboarding or within 30 days?	
64	Which of the following does the Entity gather and retain when conducting CDD? Select all that apply:	
64 a	Customer identification	
64 b	Expected activity	
64 c	Nature of business/employment	
64 d	Ownership structure	
64 e	Product usage	
64 f	Purpose and nature of relationship	
64 g	Source of funds	
64 h	Source of wealth	
65	Are each of the following identified:	
65 a	Ultimate beneficial ownership	
65 a1	Are ultimate beneficial owners verified?	
65 b	Authorised signatories (where applicable)	
65 c	Key controllers	
65 d	Other relevant parties	
66	What is the Entity's minimum (lowest) threshold applied to beneficial ownership identification?	
67	Does the due diligence process result in customers receiving a risk classification?	
67 a	If Y, what factors/criteria are used to determine the customer's risk classification? Select all that apply:	
67 a1	Product Usage	
67 a2	Geography	
67 a3	Business Type/Industry	
67 a4	Legal Entity type	
67 a5	Adverse Information	
67 a6	Other (specify)	
68	For high risk non-individual customers, is a site visit a part of your KYC process?	
68 a	If Y, is this at:	
68 a1	Onboarding	
68 a2	KYC renewal	
68 a3	Trigger event	
68 a4	Other	
68 a4a	If yes, please specify "Other"	
69	Does the Entity have a risk based approach to screening customers for Adverse Media/Negative News?	
69 a	If Y, is this at:	
69 a1	Onboarding	
69 a2	KYC renewal	

69 a3	Trigger event	
70	What is the method used by the Entity to screen for Adverse Media/Negative News?	
71	Does the Entity have a risk based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
71 a	If Y, is this at:	
71 a1	Onboarding	
71 a2	KYC renewal	
71 a3	Trigger event	
72	What is the method used by the Entity to screen PEPs?	
73	Does the Entity have policies, procedures and processes to review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
74	Is KYC renewed at defined frequencies based on risk rating (Periodic Reviews)?	
74 a	If yes, select all that apply:	
74 a1	Less than one year	
74 a2	1 – 2 years	
74 a3	3 – 4 years	
74 a4	5 years or more	
74 a5	Trigger-based or perpetual monitoring reviews	
74 a6	Other (Please specify)	
75	Does the Entity maintain and report metrics on current and past periodic or trigger event due diligence reviews?	
76	From the list below, which categories of customers or industries are subject to EDD and/or are restricted, or prohibited by the Entity's FCC programme?	
76 a	Arms, defence, military	
76 b	Respondent Banks	
76 b1	If EDD or restricted, does the EDD assessment contain the elements as set out in the Wolfsberg Correspondent Banking Principles 2022?	
76 c	Embassies/Consulates	
76 d	Extractive industries	
76 e	Gambling customers	
76 f	General Trading Companies	
76 g	Marijuana-related Entities	
76 h	MSB/MVTS customers	
76 i	Non-account customers	
76 j	Non-Government Organisations	
76 k	Non-resident customers	
76 l	Nuclear power	
76 m	Payment Service Providers	
76 n	PEPs	
76 o	PEP Close Associates	
76 p	PEP Related	
76 q	Precious metals and stones	
76 r	Red light businesses/Adult entertainment	
76 s	Regulated charities	
76 t	Shell banks	
76 u	Travel and Tour Companies	
76 v	Unregulated charities	
76 w	Used Car Dealers	
76 x	Virtual Asset Service Providers	
76 y	Other (specify)	
77	If restricted, provide details of the restriction	
78	Does EDD require senior business management and/or compliance approval?	



78 a	If Y indicate who provides the approval:	
79	Does the Entity have specific procedures for onboarding entities that handle client money such as lawyers, accountants, consultants, real estate agents?	
80	Does the Entity perform an additional control or quality review on clients subject to EDD?	
81	Confirm that all responses provided in the above Section are representative of all the LE's branches	
81 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to	
82	If appropriate, provide any additional information/context to the answers in this section.	
<b>8. MONITORING &amp; REPORTING</b>		
83	Does the Entity have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?	
84	What is the method used by the Entity to monitor transactions for suspicious activities?	
84 a	If manual or combination selected, specify what type of transactions are monitored manually	
84 b	If automated or combination selected, are internal system or vendor-sourced tools used?	
84 b1	If 'Vendor-sourced tool' or 'Both' selected, what is the name of the vendor/tool?	
84 b2	When was the tool last updated?	
84 b3	When was the automated Transaction Monitoring application last calibrated?	
85	Does the Entity have regulatory requirements to report suspicious transactions?	
85 a	If Y, does the Entity have policies, procedures and processes to comply with suspicious transaction reporting requirements?	
86	Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity?	
87	Does the Entity have a data quality management programme to ensure that complete data for all transactions are subject to monitoring?	
88	Does the Entity have processes in place to respond to Request For Information (RFIs) from other entities in a timely manner?	
89	Does the Entity have processes in place to send Requests for Information (RFIs) to their customers in a timely manner?	
90	Confirm that all responses provided in the above Section are representative of all the LE's branches	
90 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to	
91	If appropriate, provide any additional information/context to the answers in this section.	
<b>9. PAYMENT TRANSPARENCY</b>		
92	Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?	

93	Does the Entity have policies, procedures and processes to comply with and have controls in place to ensure compliance with:	
93 a	FATF Recommendation 16	
93 b	Local Regulations	
93 b1	If Y, specify the regulation	
93 c	If N, explain	
94	Does the Entity have controls to support the inclusion of required and accurate originator information in cross border payment messages?	
95	Does the Entity have controls to support the inclusion of required beneficiary information cross-border payment messages?	
95 a	If Y, does the Entity have procedures to include beneficiary address including country in cross border payments?	
96	Confirm that all responses provided in the above Section are representative of all the LE's branches	
96 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
97	If appropriate, provide any additional information/context to the answers in this section.	
<b>10. SANCTIONS</b>		
98	Does the Entity have a Sanctions Policy approved by management regarding compliance with sanctions law applicable to the Entity, including with respect to its business conducted with, or through accounts held at foreign financial institutions?	
99	Does the Entity have policies, procedures, or other controls reasonably designed to prevent the use of another entity's accounts or services in a manner causing the other entity to violate sanctions prohibitions applicable to the other entity (including prohibitions within the other entity's local jurisdiction)?	
100	Does the Entity have policies, procedures or other controls reasonably designed to prohibit and/or detect actions taken to evade applicable sanctions prohibitions, such as stripping, or the resubmission and/or masking, of sanctions relevant information in cross border transactions?	
101	Does the Entity screen its customers, including beneficial ownership information collected by the Entity, during onboarding and regularly thereafter against Sanctions Lists?	
102	What is the method used by the Entity for sanctions screening?	
102 a	If 'automated' or 'both automated and manual' selected:	
102 a1	Are internal system of vendor-sourced tools used?	
102 a1a	If a 'vendor-sourced tool' or 'both' selected, what is the name of the vendor/tool?	
102 a2	When did you last test the effectiveness (of finding true matches) and completeness (lack of missing data) of the matching configuration of the automated tool? (If 'Other' please explain in Question 110)	
103	Does the Entity screen all sanctions relevant data, including at a minimum, entity and location information, contained in cross border transactions against Sanctions Lists?	
104	What is the method used by the Entity?	

105	Does the Entity have a data quality management programme to ensure that complete data for all transactions are subject to sanctions screening?	
106	Select the Sanctions Lists used by the Entity in its sanctions screening processes:	
106 a	Consolidated United Nations Security Council Sanctions List (UN)	
106 b	United States Department of the Treasury's Office of Foreign Assets Control (OFAC)	
106 c	Office of Financial Sanctions Implementation HMT (OFSI)	
106 d	European Union Consolidated List (EU)	
106 e	Lists maintained by other G7 member countries	
106 f	Other (specify)	
107	When regulatory authorities make updates to their Sanctions list, how many business days before the entity updates their active manual and/or automated screening systems against:	
107 a	Customer Data	
107 b	Transactions	
108	Does the Entity have a physical presence, e.g. branches, subsidiaries, or representative offices located in countries/regions against which UN, OFAC, OFSI, EU or G7 member countries have enacted comprehensive jurisdiction-based Sanctions?	
109	Confirm that all responses provided in the above Section are representative of all the LE's branches	
109 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
110	If appropriate, provide any additional information/context to the answers in this section.	
<b>11. TRAINING &amp; EDUCATION</b>		
111	Does the Entity provide mandatory training, which includes:	
111 a	Identification and reporting of transactions to government authorities	
111 b	Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered	
111 c	Internal policies for controlling money laundering, terrorist financing and sanctions violations	
111 d	New issues that occur in the market, e.g. significant regulatory actions or new regulations	
111 e	Conduct and Culture	
111 f	Fraud	
112	Is the above mandatory training provided to:	
112 a	Board and Senior Committee Management	
112 b	1st Line of Defence	
112 c	2nd Line of Defence	
112 d	3rd Line of Defence	
112 e	Third parties to which specific FCC activities have been outsourced	
112 f	Non-employed workers (contractors/consultants)	
113	Does the Entity provide AML, CTF & Sanctions training that is targeted to specific roles, responsibilities and high-risk products, services and activities?	
114	Does the Entity provide customised training for AML, CTF and Sanctions staff?	
114 a	If Y, how frequently is training delivered?	
115	Confirm that all responses provided in the above Section are representative of all the LE's branches	

115 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
116	If appropriate, provide any additional information/context to the answers in this section.	
<b>12. QUALITY ASSURANCE /COMPLIANCE TESTING</b>		
117	Does the Entity have a program wide risk based Quality Assurance programme for financial crime (separate from the independent Audit function)?	
118	Does the Entity have a program wide risk based Compliance Testing process (separate from the independent Audit function)?	
119	Confirm that all responses provided in the above Section are representative of all the LE's branches	
119 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
120	If appropriate, provide any additional information/context to the answers in this section.	
<b>13. AUDIT</b>		
121	In addition to inspections by the government supervisors/regulators, does the Entity have an internal audit function, a testing function or other independent third party, or both, that assesses FCC AML, CTF, ABC, Fraud and Sanctions policies and practices on a regular basis?	
122	How often is the Entity audited on its AML, CTF, ABC, Fraud and Sanctions programme by the following:	
122 a	Internal Audit Department	
122 b	External Third Party	
123	Does the internal audit function or other independent third party cover the following areas:	
123 a	AML, CTF, ABC, Fraud and Sanctions policy and procedures	
123 b	Enterprise Wide Risk Assessment	
123 c	Governance	
123 d	KYC/CDD/EDD and underlying methodologies	
123 e	Name Screening & List Management	
123 f	Reporting/Metrics & Management Information	
123 g	Suspicious Activity Filing	
123 h	Technology	
123 i	Transaction Monitoring	
123 j	Transaction Screening including for sanctions	
123 k	Training & Education	
123 l	Other (specify)	
124	Are adverse findings from internal & external audit tracked to completion and assessed for adequacy and completeness?	
125	Confirm that all responses provided in the above section are representative of all the LE's branches	
125 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
126	If appropriate, provide any additional information/context to the answers in this section.	
<b>14. FRAUD</b>		
127	Does the Entity have policies in place addressing fraud risk?	
128	Does the Entity have a dedicated team responsible for preventing & detecting fraud?	

129	Does the Entity have real time monitoring to detect fraud?	
130	Do the Entity's processes include gathering additional information to support its fraud controls, for example: IP address, GPS location, and/or device ID?	
131	Confirm that all responses provided in the above section are representative of all the LE's branches	
131 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
132	If appropriate, provide any additional information/context to the answers in this section.	

**Declaration Statement**

Wolfsberg Group Correspondent Banking Due Diligence Questionnaire 2023 (CBDDQ V1.4)  
 Declaration Statement (To be signed by Global Head of Correspondent Banking or equivalent position holder AND Group Money Laundering Prevention Officer, Global Head of Anti- Money Laundering, Chief Compliance Officer, Global Head of Financial Crimes Compliance OR equivalent)

\_\_\_\_\_ (Financial Institution name) is fully committed to the fight against financial crime and makes every effort to remain in full compliance with all applicable financial crime laws, regulations and standards in all of the jurisdictions in which it does business and holds accounts.

The Financial Institution understands the critical importance of having effective and sustainable controls to combat financial crime in order to protect its reputation and to meet its legal and regulatory obligations.


The Financial Institution recognises the importance of transparency regarding parties to transactions in international payments and has adopted/is committed to adopting these standards.

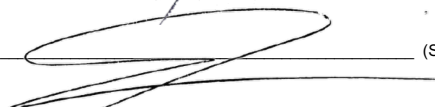
The Financial Institution further certifies it complies with / is working to comply with the Wolfsberg Correspondent Banking Principles and the Wolfsberg Trade Finance Principles. The information provided in this Wolfsberg CBDDQ will be kept current and will be updated no less frequently than every eighteen months.

The Financial Institution commits to file accurate supplemental information on a timely basis.

I, \_\_\_\_\_ (Global Head of Correspondent Banking or equivalent), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg CBDDQ are complete and correct to my honest belief, and that I am authorised to execute this declaration on behalf of the Financial Institution.

I, \_\_\_\_\_ (MLRO or equivalent), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg CBDDQ are complete and correct to my honest belief, and that I am authorised to execute this declaration on behalf of the Financial Institution.

 \_\_\_\_\_ (Signature & Date) 29 August 2023

 \_\_\_\_\_ (Signature & Date) 29 August 2023

**Annexure to FirstRand Bank Limited Wolfsberg Questionnaire: Additional Clarifying Note**

19a1d	<p><b>Nested/Downstream clearing</b></p>
	<p>Initially the nested activity was for FirstRand subsidiaries who do not have sufficient volumes to hold their own vostro accounts as this would not make business sense. For example, our operations in Lesotho. The regional downstream-stream clearing pilot programme was in USD with CITI and GBP with Lloyds Bank. African Gateway Payments now facilitated FX clearing for USD, GBP and EUR with Citi and Lloyds Bank.</p> <p>The African Gateway regional clearing service offers a holistic clearing capability to banks operating outside South Africa which combines our domestic clearing capabilities in ZAR through Rand Account services (ZAR Clearing) offering, our country domestic clearing capabilities in the Rest of Africa (Africa Subs Local Currency clearing) and finally the ability to clear USD, EUR and GBP on behalf of smaller banks in Africa which is only 7 banks currently (Foreign Currency Clearing Services), using FirstRand’s current partnership model with trusted global banking partners in foreign currency.</p> <p>Key Controls of the African Gateway Payments/Regional Clearing are:</p> <ul style="list-style-type: none"> <li>• Compliance requirements: CDD &amp; EDD Review, Country Risk assessment, In-country Visits, Transaction Monitoring, KYCC Assessment, Policy reviews, Ongoing periodic reviews.</li> <li>• Excluded Activities &amp; Sensitive Industry Matrix Review: Desirability review, identification and assessment of direct links/exposure by the Respondent Banks against our Sensitive Industry Matrix.</li> <li>• Audit Attestation: Verification of controls via a letter from the banks external auditors to confirm the adequacy of AML/CFT controls.</li> <li>• Business Case Motivation: Approval by FirstRand’s Governance Committee.</li> <li>• Counter-part Bank Clearance by Nostro Provider: The Bank’s selection criteria must be in line with Nostro provider’s jurisdictional risk appetite and existing client relationships to FirstRand.</li> </ul>
19h	<p><b>Payable Through Accounts</b></p>
	<p>Payable through Accounts are allowed by FirstRand in respect of the ZAR (vostro accounts), only by the subsidiaries or branches of the account holder. The account holder will provide us with a debit authority for the specific subsidiaries and branches. The debit authorities are reviewed on an annual basis and re-confirmed with the accountholder. In addition, the completion of a specific due diligence questionnaire on payable through accounts is obtained from the accountholders, which is reconfirmed on an annual basis.</p> <p>Payable through pertains to certain clients that are using our ZAR services where they allow their ZAR account to be used for payable through transactions – we apply enhanced due diligence on these clients and accounts. Therefore, our Nostro accounts would not be affected by these arrangements.</p> <p>Enhanced due diligence is performed in respect of the respondent banks in order to satisfy ourselves that the bank has adequate AML/CFT controls in place to perform ongoing due diligence on its underlying customers. Each respondent bank is also subjected to our internal risk model which takes into account various risk factors.</p> <p>FirstRand may, as and when required, request the respondent bank to provide relevant client due diligence data of the underlying affiliates should there be a requirement to verify or confirm certain information.</p>

47	<b>Are the Entity's policies and procedures updated at least annually?</b>
	Financial Crime policies are reviewed annually. The standards must as a minimum be reviewed every 2 years and procedures are updated after standards have been reviewed.
51 a	The record retention period for FirstRand is 7 years.
76d	<b>Extractive Industries</b>
	<p>The mining of conflict minerals, their trade and secondary resale of products/materials which contain conflict minerals, harbour extreme negative social injustice as well as facilitate war and organised crime.</p> <p>The term “conflict minerals” refers to minerals mined or extracted in zones declared as conflict zones with the aim to perpetuate political unrest, fighting and war. Minerals include blood diamonds, cassiterite, wolframite, coltan, gold ore and even petroleum. FirstRand will not finance clients who are involved in the mining, manufacture and trading of conflict minerals. FirstRand will also look to the following industry best practices, guidelines and bodies to determine effective responses to risks faced by clients, as appropriate for the related minerals and metals:</p> <ul style="list-style-type: none"> <li>• World Gold Council's Conflict Free Gold Standard;</li> <li>• Kimberly Process Certification Scheme.</li> <li>• Extractive Industries Transparency Initiative (EITI).</li> <li>• International Council on Mining and Metals (ICMM) Best Practices.</li> <li>• Responsible Jewellery Council.</li> <li>• LBMA's Guidance for Responsible Gold; and</li> <li>• Voluntary Principles for Security and Human Rights</li> </ul>
76e	<b>Gambling</b>
	<p>Relationships with unregulated/unregistered gambling entities is prohibited.</p> <p>Enhanced Due diligence is applied, in addition, each application related to gambling activities is assessed to ensure that all legislative and international best practice requirements in terms of the management of environmental and social risks associated with these activities are met as per the ESRA risk management framework. Applications will be reviewed against applicable national and provincial legislation. FirstRand Limited, as a financial institution, will limit the extent to which finance is provided to a client if gambling forms a substantial part of the clients' primary financed business activities.</p>
76g	<b>Marijuana</b>
	<p>FirstRand recognises activities related to the cultivation, manufacturing and distribution of Cannabis based products for medicinal and scientific use are deemed sensitive in nature and high-risk due to the associated reputational risk. However, it is important to note these activities are not illegal thus FirstRand does not classify them as excluded. Funding is possible subject to an enhanced due diligence through the ESRA processes, which includes a requirement that customers adhere to regional, national, international and industry best practices in this sector.</p> <p>In addition, transactions will be placed on a watch list which will receive ongoing monitoring due to ethical and reputational considerations associated with the nature of the activity.</p> <p>It is important to clarify the FirstRand (FSR) position on marijuana is specific to cannabis based and related products for medicinal and scientific use, restricting potential finance to commercial transactions.</p> <p>Note the restrictions on this financing was primarily based on concerns around supply chain oversight and the lack of control over the final destination of products, it was decided this presents a substantial risk to FSR. These restrictions are not based on the legalities as this sector is adequately regulated by the Medical Control Council predominantly through the Medicines and Related Substances Act (1965).</p>

76h	<b>MVTS/ MSB customers</b>
	<p>Relationships with unregulated/unregistered MSBs are prohibited. When entering a business relationship with a MSB, FirstRand must ensure full understanding of the MSBs legal form, structure and ownership, as well as the reasons the MSB requires the particular product or service, subject to senior management approval. Business relationships with MSBs are limited to foreign currency accounts (FCA) accounts. A FCA allows non-resident clients of FirstRand to hold balances of foreign currency. These accounts are dominated in the specific foreign currency. Due to the credit risk concerns of certain jurisdictions or clients, credit committee requires these clients who pose increased settlement risk to FirstRand to pre-fund all their transactions with FRB. Hence prior to the execution of a transaction the FCA account will be pre-funded with the transaction value. Some banks in impacted African jurisdiction have an arrangement with the MSB's to deposit the funds into their FCA account with RMB whilst giving value in the local currency to the beneficiary. In other instances, foreign NGOs wishing to send humanitarian aid also transfer funds directly to the banks FCA accounts held with RMB.</p> <p>Within South Africa, registered banks, being licensed deposit taking institutions in terms of the Banks Act 94 of 1990 (Banks Act, 1990) may engage in and provide MVTS activities and are regarded as domestic MVTS providers. Regulation 36(17) of the Regulations requires, among others, that the policies, processes and procedures of banks and controlling companies must be sufficiently robust to ensure that the bank or controlling company inter alia continuously receives relevant information relating to risk exposure incurred by any foreign operation and that every relevant foreign branch, subsidiary or operation of the bank or controlling company implements and applies AML/CFT measures consistent with the relevant FATF Recommendations issued from time to time; and the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host country are applied by the bank or controlling company.</p> <p><b>MoneyGram</b> is a product which is available to valid FNB account holders only. FNB apply very strict anti-money laundering and security procedures ensuring that customers' money is safely and securely transferred. FNB customers use MoneyGram to send money for three reasons:</p> <ul style="list-style-type: none"> <li>• Gifts (BoP code 401). South African residents and Foreign National can send money via MoneyGram as a GIFT to a beneficiary in another country.</li> <li>• Salary (BoP code 417). Foreign Nationals, like migrant workers may send a portion of their salary to beneficiaries in other countries. This option is not allowed for SA Residents.</li> <li>• Travel (BoP code 261). South African residents can send money via MoneyGram for travel purposes to their own account.</li> </ul> <p>Business status:</p> <ul style="list-style-type: none"> <li>• MoneyGram is a payment rail which the bank is integrated to via APIs to conduct Send &amp; Receive transactions. This rail is solely for the actual transactions which take place daily to settle between Sender &amp; Receiver and is separate from the settlement which takes place between FNB &amp; MoneyGram.</li> </ul> <p>PayPal is one of the world's leading digital payment platforms.</p> <p>PayPal transfers is a product which is available to FNB and non-FNB banked South African residents. FNB applies strict anti-money laundering and security procedures ensuring that customers' money is safely and securely transferred. Customers can use the FNB PayPal transfer product in two ways:</p> <ul style="list-style-type: none"> <li>• To transfer money from an FNB account to a PayPal account (Top-Up). Once the funds are in the PayPal account the customer can then buy goods and services or send money to family and friends.</li> <li>• Transfer money from a PayPal account to a South African bank account (Withdraw). The funds are received into a PayPal account for providing goods or services or transfers received from family and friends</li> </ul>



	<p>The actual payment or transfer of funds between senders and receivers happens on the PayPal platform and FNB does participate in the payment transaction. FNB facilitates the transfer of funds between a bank account and a PayPal account belonging to the same owner.</p> <p>The Top-Up and Withdraw product is only available through FNB's digital channels, which require a customer to have an FNB profile which is fully KYC'd and screened according to FNB's anti-money laundering customer screening processes on a regular basis.</p> <p>In addition to the screening performed by FNB, PayPal also screens customers for anti-money laundering and as the payment transaction occurs on their platform, they perform transaction screening.</p>
<b>76l</b>	<b>Nuclear Power</b>
	<p>FirstRand has identified the arms/defence industry as high-risk with regards to credit risk, reputational risk, sanctions risk and anti-bribery and corruption, which requires specific policy positioning. Every application related to weapons, ammunition, defensive and protective clothing or any other equipment that can be linked to the arms industry, is subjected to an enhanced due diligence (ESRA) process.</p> <p>FirstRand will not provide financial services or financial products to industries involved in the development, manufacturing, maintenance, stockpiling, transfer, use, testing and production of, or trade in nuclear, chemical, biological or other weapons of mass destruction, landmines, cluster bombs (including cluster munitions in violation of the international convention on cluster munitions) or any equipment designed to be used as an instrument of torture and/or the delivery systems of such instruments</p>
<b>76r</b>	<b>Adult Entertainment/Red Light Business</b>
	<p>FirstRand will not finance clients where funds will be used for any purpose related to pornographic activity. For purposes of this position statement, pornography is understood to be sexually explicit material (verbal or pictorial) or erotic material that is primarily designed to produce sexual arousal in viewers. It is important to distinguish here between sexually explicit material that is wholly or primarily designed to produce sexual arousal (i.e., whose only or overriding aim is to produce sexual arousal) and material whose aim is to do this to make some other artistic or political point. Pornographic activity may use a variety of media including books, magazines, postcards, photos, sculpture, drawing, painting, animation, sound recording, film, video and video games.</p>
<b>76x</b>	<b>Virtual/Digital Currencies</b>
	<p>FirstRand has limited exposure to Virtual Currency providers and exchanges.</p> <p>FirstRand has previously made an appetite decision to only offer operational bank accounts to VC providers and exchanges, in respect of salary and operational payments. Monitoring is in place for customers or entities buying or selling VCs in the normal course of business, in respect of financial crime and Excon.</p>
<b>107a</b>	For clarification, FirstRand updates Customer screening systems the same day or the next day and not 2 business days later. This is not an option on the dropdown list.
<b>107b</b>	For clarification, FirstRand updates Transactional screening systems the same day or the next day and not 2 business days later. This is not an option on the dropdown list.
<b>112f</b>	For clarification, Contractors who do not have access to our systems, clients and transactions data and contracted to the bank for a period of 3 months or less, are not required to do training.