FOREIGN CORRESPONDENT BANKING: RISK APPETITE STATEMENT

JUNE 2026

1. FINANCIAL CRIME RISK APPETITE

Citi has no appetite for:

- Intentional, wilfully negligent breaches of law, regulation or policy applicable to Financial Crime Risk.
- Repeated unintentional or accidental breaches of law, regulation or policy applicable to Financial Crime Risk.

2. ANTI-BRIBERY & CORRUPTION RISK APPETITE

Citi has no appetite for providing or receiving anything of value from/to Public Officials or clients to obtain an improper advantage in return, including obtaining or retaining business for, or on behalf, of Citi. Citi expects its clients to have policies, procedures and a program in place to comply with Anti-Bribery & Corruption laws and regulations in their jurisdiction, as well as the jurisdictions in which their affiliates, branches and customers operate.

3. ANTI-MONEY LAUNDERING RISK APPETITE:

Citi has no appetite for:

- Dealing in countries deemed state sponsors of terrorism by the U.S. State Department or conducting business in jurisdictions and with any entities, including financial institutions subject to Special Measures under Section 311 of the USA PATRIOT Act, including those under a Notice of Proposed Rulemaking (NPRM), the FEND off Fentanyl Act 21 U.S.C. 2313a, or equivalent.
- Facilitating any entity or individual, which seek to launder proceeds, obtained from financial crime in any form including drug trafficking, tax evasion, illegal arms trafficking, human trafficking, etc.
- Facilitating any entity or individual, which seek to finance terrorism.

Specific to Special Measures, Citi has no appetite to:

- Open or maintain correspondent or payable-through accounts prohibited under Section 311
- Process transactions involving entities or jurisdictions subject to Section 311 prohibitions
- Engage in business designed to circumvent or evade Section 311 special measures

Citi expects its clients to have anti-money laundering (AML) programs that include customer due diligence, enhanced due diligence, and suspicious and prohibited transaction monitoring and reporting policies as well as surveillance systems to monitor such activity. The AML program should be aligned to their risk appetite and adequately mitigate risk.

4. SANCTIONS RISK APPETITE

Citi has no appetite:

- For establishing or actively operating a customer or counterparty relationship with a directly designated entity or individual present on the UN Security Council Sanctions List; the Consolidated List of EU Financial Sanctions; the US OFAC Specially Designated Nationals and Blocked Persons List (OFAC List) or Correspondent Account or Payable-Through Account Sanctions List (CAPTA List); or the UK's Sanctions List; or entities majority-owned[1] or controlled by such persons[2].
- For establishing or actively operating a customer or counterparty relationship with an entity or individual living or operating in a jurisdiction subject to OFAC comprehensive sanctions.
- To execute transactions involving, directly or indirectly, any US, EU, or UK sanctioned person, jurisdiction, or vessel.
- For providing financial services relating to any such persons or vessels.
- To execute transactions or financial services intended to circumvent or evade US, UK, UN, or EU sanctions.

Citigroup Inc., its subsidiaries, and affiliates, including Citibank, N.A., (collectively, "Citi") are required to comply with applicable sanctions laws and regulations ("Sanctions") imposed and administered by the United States, the United Kingdom, United Nations, and the European Union as well as by other sanctions authorities of each jurisdiction where Citi operates.

Citi requires its correspondent banking clients to screen their transactions against OFAC lists as well as any list(s) issued by sanctions authorities of the jurisdiction where the financial activity is booked and the jurisdiction of the currency used.

Citi expects its clients to screen their customers against all lists above as well as any list issued by sanctions authorities of the jurisdiction where the financial activity is booked. Citi also expects clients to refrain from sending to or through Citi prohibited transaction requests relating to any person (or entities majority-owned[1] or controlled by such persons[2]), or jurisdiction subject to sanctions, particularly US, EU, UN, or UK sanctions.

[1] Under the U.S. Department of the Treasury's OFAC regulations, a "majority-owned entity" is defined by the 50 Percent Rule. This rule stipulates that any entity owned 50% or more, directly or indirectly, in the aggregate by one or more blocked persons (such as those on the SDN List) is itself considered blocked, even if not explicitly listed.

[2] The Office of Financial Sanctions Implementation (OFSI) expects firms and individuals to fully consider the risks of an entity being owned or controlled by a UK Designated Person ("UK DP"). Asset freeze measures and some financial services restrictions will apply to entities that are owned (more than 50%) or controlled, directly or indirectly, by a designated person. Those entities might not be designated in their own right, so their names might not appear on the UK sanctions list. However, those entities are similarly subject to financial sanctions. Under EU law, entities owned (50% or more) or controlled by a person or entity on the Consolidated Financial Sanctions List are automatically subject to asset freezes and prohibitions, even if not explicitly listed by name. This "50% rule" covers directly and indirectly owned companies, including subsidiaries and joint ventures.

5. RISK FACTORS - CLIENT

Citi will not do business with, or process payments on behalf of, the following entities:

- Shell banks, defined as banks that do not maintain a physical presence in any country, and are not affiliated with any bank that has a physical presence in any country.
- Clients with bearer share ownership (no new accounts will be opened for existing clients with bearer share ownership).

Accounts will not be set up for the purpose of:

- Allowing the client's (bank) customers to directly transact through the account in support of their business activities (Payable Through Accounts).
- Supporting any business engaged in activity prohibited by applicable law or regulation including but not limited to the following: illegal arms, human trafficking or narcotics dealers, illegal pornography.
- Processing transactions that are restricted or unlawful under the Unlawful Internet Gambling Enforcement Act ("UIGEA") and Regulation GG of the Federal Reserve Board, 12 C.F.R. Part 233 (for US$ denominated accounts).

6. RISK FACTORS – PAYMENT TRANSPARENCY

Tackling financial crime and terrorist financing continues to be a high priority for regulators, who are taking steps to improve the transparency and traceability of payments. FATF Recommendation 16 specifies that banks should provide information about beneficiaries as well as originators in their outgoing messages.

Citi expects its clients:

- Apply high payment transparency standards, in full compliance with FATF Recommendation 16, applicable national laws and regulations.
- Have, as part of their monitoring processes, a risk-based method to identify incomplete or missing information or fields with meaningless data.
- To reject payments received where complete payment information is not received or provided upon request.

7. RISK FACTORS – GEOGRAPHIES

Citi has concerns on the certain geographies and therefore has little to no appetite to process payments for its respondent institutions involving these jurisdictions.

Citi expects its client to refrain from using Citi product and services to process payments to or from listed jurisdictions in Annex 1.

8. RISK FACTORS – INDUSTRIES

Citi has **No Appetite** for:

- Illegal Weapons.
- Adult Entertainment.
- Cannabis.
- Casinos and other gambling entities (excluding state sponsored lotteries).
- Unregulated/non-registered Charities/NGOs.
- Illegal mining.

Citi expects its clients to refrain from using Citi products and services to process payments involving the above listed industries.

Citi has **Limited Risk Appetite** for:

- Downstream Correspondent Banking (aka Nesting or Tiering) including:
  - Payment Intermediaries.
  - Virtual Currency (VC) issuers, administrators, miners, and exchanges.
- Legal Weapons and associated industries.

Citi expects its clients to seek approval prior to sending such activity though accounts with Citi.

The following industries may present elevated risk, and additional assessment may be required:

- Travel and tour companies.
- Precious metal dealers.
- Extractive industries.
- Companies located in free trade zones or equivalent.
- Off-Shore Financial Centers / Off-Shore Bookings.
- Embassies / Consulates / Military attachés.
- Government owned enterprises in countries which score highly on the corruption index.
- Crowdfunding.

Citi expects its clients to disclose business with the above high-risk industries, and any other industries which the client considers high risk even if not listed above, as part of due diligence discussions at the time of onboarding and renewal.

Citi may seek additional information from clients via RFI for activity which we deem concerning in nature. Citi expects its clients to respond to such RFIs in a comprehensive and timely manner. In cases of insufficient response, Citi reserves the right to reject any payments of concern to us and issue a Client Restriction Notice to prohibit clients from sending these flows through Citi.

Annex 1: Geographies for which Citi has little to no risk appetite:

- Afghanistan
- Belarus
- Crimea
- Cuba
- Donetsk People's Republic (DNR)
- Equatorial Guinee
- Iran
- Kherson
- Luhansk People's Republic (LNR)
- Myanmar
- North Korea
- Russia
- Syria
- Venezuela
- Yemen
- Zaporizhzhia