OCTOBER 2023

J.P. MORGAN POLICY REGARDING THE USE OF YOUR ACCOUNTS AND SERVICES

Compliance with laws that are intended to combat money laundering and terrorist financing and fraud is a top priority for J.P. Morgan globally. We view our clients as partners in ensuring that accounts at J.P. Morgan are operated in full compliance with applicable laws and regulations and sound risk management practices. J.P. Morgan has adopted the following policy to supplement the terms and conditions governing the use of your accounts and services ("Account Documentation"), which you use to process payments for your clients or other third parties (your "J.P. Morgan Accounts"). Our policy, which is focused on the steps that we require you to take to promote compliance, is set forth below.

1.General. From time to time, our relationship or compliance teams will request information from you regarding your organization and your business to fulfill our "know your customer" responsibilities. Our relationship or compliance teams may also contact you to: (a) request information about your direct customers; (b) request information about transactions in your J.P. Morgan Accounts and the parties to the transactions; (c) share pertinent information and best practices; and (d) direct you to make changes to the activity in your J.P. Morgan Accounts, including to cease and desist from using your J.P. Morgan Accounts for particular types of transactions, for transactions involving particular parties or for transactions with certain characteristics. It is essential that you provide complete responses to our requests and/or comply with our directions within the timeframes we may specify.

Because the fight against money laundering, terrorist financing and other financial crimes is so important, we require you, to the extent legally permissible, to report activity in your J.P. Morgan Accounts that you have identified as warranting additional review by virtue of it being illegal, illegitimate, unusual, suspicious or high risk, or on the basis of any factor that indicates the activity may be outside of the risk tolerance detailed below or otherwise notified to you. You may report this activity to your relationship manager in writing (including by e-mail) or by telephone. J.P. Morgan Compliance may contact you for additional information. Note that this reporting requirement is in addition to any reporting requirements you may be subject to under laws and regulations applicable to you.

Furthermore, fraud perpetrated against financial and payment institutions and their customers is increasing including through the use of malicious computer software and spurious communications. Payment orders and other instructions received by J.P. Morgan with respect to your accounts via SWIFT, J.P. Morgan Access®, J.P. Morgan Host-to-Host, J.P. Morgan Treasury Services API or other channels are authenticated using the applicable security procedure. Because authenticated payment orders and other instructions will be deemed to be authorized by you, it is your responsibility to ensure that the security procedures and your funds transfer operations and systems are safeguarded and protected from compromise.

Additionally for users of SWIFT the following applies: As SWIFT authentication is relied upon by J.P. Morgan to authenticate all payment orders and other instructions received by J.P. Morgan via SWIFT, it is critical that our customers safeguard their SWIFT credentials and relevant SWIFT environments and infrastructure from compromise to prevent fraudulent activity on their accounts. The Customer Security Controls Framework ("CSCF") established by SWIFT sets forth user security controls to prevent such compromise. Accordingly, if you are a SWIFT user, absent a written exception granted by J.P. Morgan, J.P. Morgan requires you to comply with the mandatory controls set forth in SWIFT's CSCF as it may be amended, modified or updated from time to time.

You are expected to maintain appropriate licensing and registration as required by applicable law in connection with the activity conducted through your J.P. Morgan Accounts in each jurisdiction in which you do business (e.g., money transmission, payment services) and in which J.P. Morgan maintains your J.P. Morgan Accounts, and to otherwise comply with all applicable laws and regulations in such jurisdictions. You are required to comply with all applicable rules and regulations governing each payment method you utilize as well as any payment formatting requirements stipulated by J.P. Morgan. To the extent there is any inconsistency between a funds transfer financial messaging or formatting standard and the governing law set forth in the Account Documentation, the governing law set forth in the Account Documentation will govern.

2. Transactions That Must Not Be Processed Through Your J.P. Morgan Accounts. Your J.P. Morgan Accounts must not be used to process transactions with the following characteristics:

A. Payments that appear to relate to any form of illegal activity, including without limitation, fraud, money laundering, terrorist financing, human trafficking, political corruption, and illegal wildlife trafficking;

B. Payments that do not appear to have a legitimate purpose;

C. Payments that involve the use of an Informal Value Transfer System, as defined in U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Advisory FIN-2010-A011, such as hawalas or money transmitters who do not comply with applicable registration or licensure requirements;

D. Payments that would violate, or cause J.P. Morgan to violate, economic sanctions imposed or enforced by the United Nations, the United States, the European Union or any Member State, the United Kingdom, or any other applicable sanctions;

E. Payments that would violate, or cause J.P. Morgan to violate, export controls, and other economic restrictions imposed by various governments.

F. Payments arising from, or related to, transactions in Russian-origin oil or in other Russian-origin oil or petroleum products (as defined under HS codes 2709 and 2710), irrespective of their price.

G. Payments that appear to circumvent currency controls;

H. Payments involving any Virtual Asset Service Providers (VASPs)[1] as your direct customers, including virtual currency exchanges, administrators and miners if such customers:

i) Are in a jurisdiction with strategic deficiencies as designated by the FATF; or

ii) Are not compliant with applicable regulatory money transmission licensing, money service business registration, and AML program requirements within the local jurisdiction; and/or

iii) Do not have an AML program generally consistent with FATF standards

I. Payments involving unlawful internet gambling;

J. Payments involving shell banks, as defined in Section 1010.605 of Title 31 of the U.S. Code of Federal Regulations;

K. Payments involving bearer share companies (and operating as such), except for those that are publicly traded on a recognized exchange;

L. Payments associated with payable through accounts;

M. Payments involving third-party payment processors or money transmitters that provide downstream processing for MSBs, financial institutions and Payment Service Providers that do not have an AML and Sanctions program in place.

We expect that your transaction monitoring controls will ensure that your J.P. Morgan Accounts are not used for transactions in these categories and, as provided in the Account Documentation, we may reject any such transactions and we reserve all our rights to take any additional action as provided in the Account Documentation and this policy.

3. Transactions That Can Only Be Processed Through Your J.P. Morgan Accounts Subject To Your Implementation of Certain Controls. Certain other types of transactions may also present a high level of financial compliance risk. Our expectation is that you will not process the types of payments listed below through your J.P. Morgan Accounts unless your "know your customer"/anti-money laundering policies and your transaction monitoring controls are commensurate with the nature, scale, size and complexity of your business and can assure that transactions in these categories will not violate applicable laws and regulations and/or present an unacceptable level of AML or other compliance risk. To the extent that your policies and controls are not capable of assuring that payments in the categories below will not violate applicable laws and regulations or present an unacceptable level of AML or other compliance risk, please do not use your J.P. Morgan accounts for such transactions.

A. Payments involving arms and munitions, microchips, and/or other components that have dual use potential, but are not otherwise subject to export control requirements[2];

B. Payments involving precious metals dealers that purchase metals from pawnbrokers and other secondary sources;

C. Payments involving shipping and general trading companies operating in free trade zones;

D. Payments involving tour and travel companies including but not limited to companies where there is a potential nexus to sanctions exposure;

E. Payments involving charities;

F. Payments involving used motor vehicles dealers or auctions;

G. Payments involving auctions including online auctions;

H. Payments related to crowdfunding platforms;

[1] As defined by the Financial Action Task Force (FATF) Recommendations on the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (updated June 2021).

[2] See Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts, available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf.; *See* NTE 2023/08: Russia sanctions – Trade sanctions circumvention, https://www.gov.uk/government/publications/notice-to-exporters-202308-russia-sanctions-trade-sanctions-circumvention/nte-202308-russia-sanctions-trade-sanctions-circumvention

I. Payments related to transactions in penny stocks or microcap securities;

J. Payments involving transactions designed to achieve a particular tax treatment;

K. Payments involving embassies, consulates and diplomatic missions;

L. Payments involving economic citizenship or citizenship by investment programs;

M. Payments involving government scholarship programs where the beneficiary is not an educational institution;

N. Payments involving relationships established with universities or students for online tuition solutions;

O. Payments involving adult oriented services (where such services are permitted by law); and

P. Payments involving online or in person gambling services (e.g. daily fantasy sports, online poker, casinos, gambling machines or the like).

4. Transactions Types That Require Notification and Approval by J.P. Morgan. For the following activity that in our assessment presents a higher risk of money laundering, terrorist financing or other financial crimes and involves the introduction of additional entities routing third party activity through your J.P. Morgan Accounts, we require you to notify your Relationship Manager and receive affirmative consent prior to processing this activity:

A. Payments involving downstream processing for correspondent banks, MSBs, financial institutions, VASPs[3] and Payment Service Providers that are not otherwise prohibited under Sections 2.H. and 2.M of this policy.

In addition, as part of that notification process J.P. Morgan requires that you subject these flows to your Enhanced Due Diligence controls, which should include at a minimum the following: (i) tailored transaction monitoring scenarios for downstream/nested activity, (ii) periodic due diligence reviews of the downstream entity, and (iii) an established process for obtaining payment purpose details through a Requests for Information ("RFI").

You may direct any questions concerning this policy to your Relationship Manager. Please take the necessary steps to assure compliance, as failure to comply with this policy could lead to rejection of payments and/or closure of your accounts.

[3] As defined by the FATF Recommendations on the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (updated June 2021).