ESSENTIAL INFORMATION PROSPECTUS

BRAZIL

[LB20220801_V1.7_02_03_21]

This prospectus ("Prospectus") contains general information regarding demand deposit accounts ("Accounts") held by the customer ("Customer"), in Brazil, with Banco J.P. Morgan S.A. ("Bank") and briefly describes the basic rules applicable to the operation of the Accounts, its existing risks and security measures adopted by the Bank, including in the event of loss or theft of the Customer's credentials. The Customer and the Bank may, at their discretion, negotiate certain terms and conditions of the Account Documentation (as defined below). This Prospectus is part of the Account Documentation and, in the event of any discrepancy between this Prospectus and the Account Documentation, the Account Documentation shall prevail.

1. Basic Rules

1.1. Engagement. The terms, conditions and general information applicable to the Accounts and to the services related to the Accounts provided by the Bank ("Services") are set forth in the respective documents, including an instrument that sets forth the terms and conditions applicable to the Account, addenda, service terms applicable to a certain Service, signature cards, application forms, registration form and other applicable documents, as amended from time to time (jointly "Account Documentation"). The Account Documentation may be delivered, made available and/or made accessible to the Customer by ordinary mail or courier at the address of the Customer provided to the Bank, or by facsimile transmission, electronic means and channels (including SWIFT message, emails and by posting on a Bank website), or by such other means as the parties agree upon from time to time.

1.2. Onboarding. The Bank may periodically request, from the Customer and third parties, information and documents that enable the identification of the Customer, the person(s) authorized to act on its behalf in relation to the Accounts and Services ("Authorized Persons"), and any third parties that have access to the Accounts ("Third Parties"), such as names, addresses, dates of birth, final beneficiaries, among others, as a way of preventing money laundering and the financing of terrorism in compliance with its internal policies, the applicable legislation and/or regulations.

1.3. Transactions. Authorized Persons and Third Parties, as applicable, may provide instructions to the Bank ("Instructions") involving, for example, execution of transactions, granting of access, provision of information, among others.

As made available by the Bank from time to time, Accounts may receive or transfer funds through mechanisms provided and/or accepted by the Bank, such as wire transfers (*Transferência Eletrônica Disponível* – TED and *Documento de Ordem de Crédito* – DOC), collection slips (*boletos*), bank cashier's check and RTP, during the cut-off limits disclosed and periodically updated by the Bank on its website. The Bank does not provide check books and banking cards for the Accounts, nor does it accept transactions of any type in cash.

1.4. Interest and Investments. Accounts, funds and items deposited by the Customer with the Bank are not interest-bearing, shall yield no interest nor be subject to any monetary adjustment index. However, if the Customer is interested, it may contract certain types of investments, including Bank Deposit Certificates, as made available by the Bank.

1.5. Fees. The Bank may charge fees for the existence of the Accounts and the provision of the Services, as defined in the

PROSPECTO DE INFORMAÇÕES ESSENCIAIS

BRASIL

Este prospecto ("Prospecto") contém as informações gerais relativas às contas de depósito à vista ("Contas") mantidas pelo cliente ("Cliente"), no Brasil, junto ao Banco J.P. Morgan S.A. ("Banco") e explicita, de forma sintética, as regras básicas de funcionamento das Contas, os riscos existentes e as medidas de segurança adotadas pelo Banco para fins de movimentação das Contas, inclusive em caso de perda, furto ou roubo de credenciais do Cliente. O Cliente e o Banco podem, à sua discricionaridade, negociar determinados termos e condições da Documentação de Conta (conforme definido abaixo). Este Prospecto é parte integrante da Documentação de Conta e, em caso de divergência entre este Prospecto e a Documentação de Conta, a Documentação de Conta deverá prevalecer.

1. Regras Básicas

1.1. Contratação. Os termos, condições e informações gerais aplicáveis às Contas e aos serviços relacionados à Conta prestados pelo Banco ("Serviços") estão previstos nos respectivos documentos, incluindo instrumento que prevê os termos e condições da Conta, adendos, termos de serviços aplicáveis a determinado Serviço, cartões de assinatura, formulários, ficha cadastral e demais documentos aplicáveis, conforme alterados de tempos em tempos (conjuntamente "Documentação da Conta"). A Documentação da Conta pode ser enviada e/ou disponibilizada ao Cliente via correio ou *courier* no endereço do Cliente fornecido ao Banco, por fax e outros canais eletrônicos (incluindo mensagem SWIFT, *e-mails* e postagens em um site do Banco), ou por outras formas acordadas periodicamente entre as partes.

1.2. Cadastro. O Banco pode solicitar periodicamente, ao Cliente e a terceiros, informações e documentos que permitam a identificação do Cliente, da(s) pessoa(s) autorizada(s) a agir em seu nome com relação às Contas e Serviços ("Pessoas Autorizadas"), e de eventuais terceiros que tenham acesso às Contas ("Terceiros"), tais como nomes, endereços, datas de nascimento, beneficiários finais, dentre outros, como forma de prevenir a lavagem de dinheiro e o financiamento do terrorismo em atendimento às suas políticas internas, legislação e/ou regulamentação aplicáveis.

1.3. Movimentação. Pessoas Autorizadas e Terceiros, conforme aplicável, podem fornecer instruções ao Banco ("Instruções") envolvendo, por exemplo, movimentação de recursos, concessão de acessos, fornecimento de informações, dentre outros.

Conforme disponibilizado pelo Banco de tempos em tempos, as Contas podem ser movimentadas por meio de mecanismos oferecidos e/ou aceitos pelo Banco, como TED, DOC, boleto, cheque administrativo e PIX, observados os horários de corte e os horários limite publicados e atualizados periodicamente pelo Banco em sua página da internet. O Banco não fornece talonário de cheques e cartões magnéticos para as Contas e tampouco permite movimentação de recursos em espécie.

1.4. Remuneração da Conta e Investimentos. As Contas, recursos e itens depositados pelo Cliente junto ao Banco não são remunerados, não rendem juros e não estão sujeitos a nenhum índice de correção monetária. Contudo, caso o Cliente tenha interesse, poderá contratar certas modalidades de investimentos, incluindo Certificados de Depósito Bancário, conforme disponibilizado pelo Banco.

1.5. Tarifas. O Banco pode cobrar tarifas em virtude da existência das Contas e da prestação dos Serviços, conforme estipulado na tabela de tarifas e encargos

fees and charges chart disclosed and periodically updated by the Bank on its website.

1.6. Bank Secrecy and Data Protection. The Bank may use and disclose Customer's information as provided in the Account Documentation. In addition, the Bank processes information about the Customer, as provided in the Privacy Policy for Brazil (https://www.jpmorgan.com/country/br/pt/privacy).

1.7. Termination. The Bank or the Customer may terminate the Accounts and/or the Services (i) upon prior written notice sent to the other party at least 30 (thirty) days in advance; or (ii) immediately, upon written notice to the other party, in the event of breach of contract, inability to meet debts as they become due, legal requirement or court order, engagement in activities that are inconsistent with the terminating party's policies, among other events provided for in the Account Documentation.

The Bank shall have no obligation to terminate the Account while the Customer has a debt arising from the Account, the Services and/or any contractual obligation set forth in the Account Documentation.

2. Existing Risks

2.1. Fraud and Security. The Services are subject to fraud and security risks, for example fraudulent transactions, theft and/or data leakage. These risks are mitigated by the security procedures applicable to each Service adopted by the Bank, which must also be adopted by the Customer, as applicable.

2.2. Insolvency. There is a risk of insolvency of the Bank, which is mitigated by the Bank's financial stability and by the existence of the Credit Guarantee Fund (FGC), which, upon intervention or liquidation by the Central Bank of Brazil, guarantees the recovery of certain balances and investments held/made by the Customer with the Bank, up to the limit and in accordance with the rules defined in applicable legislation and regulations.

3. Security Measures

3.1. Security Procedures. The Bank may require the Customer to use algorithms or other identification codes, words or numbers, encryption, call back procedures or other similar security devices to verify the authenticity of Instructions received. For example, whenever the Customer sends the Bank Instructions for the transfer of funds in digital format, such Instructions must be transmitted to the e-mail address indicated in writing by the Bank, and the Customer must, immediately after sending such Instructions, call the Bank to confirm its receipt.

3.2. Fraud Prevention Procedures. The Bank has resources and tools that can help protect the Customer from potential cyber threats, as provided on the Fraud Solutions (https://www.jpmorgan.com/commercial-banking/solutions/treasury-payments/fraud-solutions) and J.P. Morgan Access Security Center (https://www.jpmorgan.com/commercial-banking/insights/cybersecurity) pages. In addition to these tools, other ways for the Customer to mitigate and handle fraud risks include:

- be careful when reviewing and confirming e-mail payment Instructions, especially those that contain new beneficiary banks, names and account numbers;
- do not hesitate to call the beneficiary information provider if it receives any abnormal e-mail requests involving payment Instructions;

publicada e atualizada periodicamente pelo Banco em sua página da internet.

1.6. Sigilo Bancário e Proteção de Dados. O Banco pode utilizar e divulgar informações do Cliente conforme previsto na Documentação da Conta. Além disso, o Banco trata informações sobre o Cliente, conforme previsto na Política de Privacidade para o Brasil (https://www.jpmorgan.com/country/br/pt/privacy).

1.7. Encerramento. O Banco ou o Cliente podem encerrar as Contas e/ou os Serviços (i) mediante notificação prévia enviada por escrito à outra parte com, no mínimo, 30 (trinta) dias de antecedência; ou (ii) imediatamente, mediante notificação por escrito à outra parte, em caso de violação contratual, incapacidade de honrar o pagamento de dívidas, exigência legal ou ordem judicial, envolvimento em atividades inconsistentes com as políticas da parte rescisora, dentre outras hipóteses previstas na Documentação da Conta.

O Banco não terá qualquer obrigação de encerrar a Conta enquanto o Cliente possuir uma dívida decorrente da Conta, dos Serviços e/ou de qualquer obrigação contratual prevista na Documentação da Conta.

2. Riscos Existentes

2.1. Fraude e Segurança. Os Serviços estão sujeitos a riscos de fraude e segurança, por exemplo a ocorrência de transações fraudulentas, roubo e/ou vazamento de dados. Estes riscos são mitigados pelos procedimentos de segurança aplicáveis a cada Serviço adotados pelo Banco, os quais também devem ser adotados pelo Cliente, conforme aplicável.

2.2. Insolvência. Existe risco de insolvência do Banco o qual é mitigado pela higidez financeira do Banco e pela existência do Fundo Garantidor de Crédito (FGC), o qual, em casos de intervenção ou de liquidação pelo Banco Central do Brasil, garante a recuperação de determinados saldos e investimentos mantidos/realizados pelo Cliente junto ao Banco, até o limite e conforme as regras definidas na legislação e regulamentação aplicáveis.

3. Medidas de Segurança

3.1. Procedimentos de Segurança. O Banco pode exigir que o Cliente utilize algoritmos ou outros códigos, palavras ou números de identificação, criptografia, procedimentos de chamadas de retorno (*call back*) ou outros dispositivos de segurança similares para verificar a autenticidade de Instruções recebidas. Por exemplo, sempre que o Cliente enviar ao Banco Instruções para transferência de fundos em via digitalizada, tais Instruções deverão ser transmitidas para o endereço de e-mail indicado por escrito pelo Banco, e o Cliente deverá, imediatamente após enviar tais Instruções, ligar para o Banco para confirmar o seu recebimento.

3.2. Procedimentos de Prevenção à Fraude. O Banco tem recursos e ferramentas que podem ajudar a proteger o Cliente de possíveis ameaças cibernéticas, conforme previsto nas páginas *Fraud Solutions* (https://www.jpmorgan.com/commercial-banking/solutions/treasury-payments/fraud-solutions) e *J.P. Morgan Access Security Center* (https://www.jpmorgan.com/commercial-banking/insights/cybersecurity). Além dessas ferramentas, outras formas do Cliente mitigar e lidar com riscos de fraude incluem:

- estar atento ao revisar e confirmar as Instruções de pagamento por e-mail, especialmente aquelas que contêm novos bancos beneficiários, nomes e números de contas;
- não hesitar em ligar para o provedor das informações do beneficiário se receber qualquer

- do not to send Instructions requested by third parties quickly or due to emergencies, as requests of this nature can be fraudulent, since fraudsters usually create a sense of urgency for people to act quickly;

- regularly check Accounts activities for suspicious transactions;

- forward suspicious emails regarding J.P. Morgan Access to phishing@jpmchase.com, adding “J.P. Morgan Access” in the subject line; and

- contact the J.P. Morgan Access Service Center if it believes that it has been a victim of fraud or that its access credentials have been compromised, for example in the event of loss or theft, so that the Bank can analyze the situation and take the necessary measures.

solicitação de e-mail anormal envolvendo Instruções de pagamento;

- não enviar Instruções solicitadas por terceiros rapidamente ou devido a emergências, pois solicitações desta natureza podem ser fraudulentas, já que fraudadores costumam criar senso de urgência para que as pessoas ajam rapidamente;

- verificar regularmente a atividade das Contas em busca de transações suspeitas;

- encaminhar e-mails suspeitos em relação ao J.P. Morgan Access para phishing@jpmchase.com, adicionando “J.P. Morgan Access” na linha de assunto; e

- contatar a Central de Atendimento do J.P. Morgan Access se acreditar que foi vítima de fraude ou que suas credenciais de acesso foram comprometidas, por exemplo em caso de perda, roubo ou furto, para que o Banco possa analisar a situação e tomar as providências necessárias.