Política de Serviços de Transferência de Criptoativos

Versão Portuguesa >> Página 3

Crypto-Assets Transfer Services Policy

English Version >> Page 21

Disclaimer:

Em caso de divergência entre as versões, as Partes declaram que prevalece o disposto na versão portuguesa.

In the event of any discrepancy between the versions, the Parties hereby declare that the provisions set forth in the Portuguese version shall prevail

Contents

1. Introdução 3
2. Enquadramento 3
2.1 Âmbito e Objetivo 3
2.2 Definições 3
2.3 Enquadramento legal 4
3. Documento referenciados 4
4. Informação pré-contratual 4
5. Termos e condições gerais dos serviços de transferência de criptoativos 6
6. Informação relativa a transferências 6
7. Receção de ordens, prazos-limite para receção de ordens, prazos de execução e irreversibilidade das transferências 8
8. Execução, rejeição, devolução ou suspensão de ordens de transferência 11
9. Responsabilidade do Banco 14
10. Travel Rule 18
11. Aprovação e revisão 19
1. Introduction 21

1. Introdução

A presente política de serviços de transferência de criptoativos ("**Política**") foi aprovada pelo Conselho de Administração do Bison Bank, S.A. ("**Bison Bank**" ou **"Banco"**) nos termos e para os efeitos do artigo 82.º do Regulamento (UE) n.º 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023 ("**MiCA**"), das Orientações da ESMA relativas a serviços de transferência de criptoativos (ESMA35-1872330276-2032, de 26 de fevereiro de 2025), do Regulamento (UE) n.º 2023/1113 do Parlamento Europeu e do Conselho, de 31 de maio de 2023 ("**TFR II**"), e das Orientações da EBA (EBA/GL/2024/11), de 4 de julho de 2024, relativas às transferências de fundos e certas transferências de criptoativos ao abrigo do Regulamento (UE) 2023/1113 ("**Orientações TFR**").

A presente Política estabelece os procedimentos relativos ao cumprimento dos requisitos aplicáveis ao Banco, enquanto prestador de serviços de criptoativos que oferece serviços de transferência de criptoativos em nome de clientes, incluindo os direitos dos clientes no contexto desses serviços de transferência de criptoativos.

2. Enquadramento

2.1 Âmbito e Objetivo

Esta Política aplica-se a todos os serviços de transferência de criptoativos em nome de clientes, conforme definidos no MiCA[1], i.e., os serviços de transferência, em nome de uma pessoa singular ou coletiva, de criptoativos (EMTs ou Outros que não EMTs ou ARTs) de um endereço ou conta de registo distribuído para outro.

Para efeitos da presente Política, tecnologia de registo distribuído significa uma tecnologia que permite o funcionamento e a utilização de registos distribuídos ("**DLT**")[2].

A presente Política é aplicável aos colaboradores e aos membros do Conselho de Administração e da Comissão de Auditoria do Banco.

2.2 Definições

[1] Artigo 3.º, n.º 1, alínea 26) do MiCA.
[2] Artigo 3.º, n.º 1, alínea 1) do MiCA.

Para efeitos da presente Política, são considerados "clientes" todas as pessoas singulares ou coletivas que (i) sejam clientes atuais, (ii) sejam potenciais clientes (i.e., em relação aos quais o Banco procura iniciar uma relação contratual), ou (iii) tenham sido clientes que já terminaram a sua relação contratual com o Banco, mas em relação aos quais esta ainda se mantém vinculada por obrigações pós-contratuais, fiduciárias ou similares.

2.3 Enquadramento legal

- Regulamento (UE) n.º 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023 ("**MiCA**")
- Orientações da ESMA relativas a serviços de transferência de criptoativos (ESMA35-1872330276-2032, de 26 de fevereiro de 2025)
- Regulamento (UE) n.º 2023/1113 do Parlamento Europeu e do Conselho, de 31 de maio de 2023 ("**TFR II**")
- Orientações da EBA (EBA/GL/2024/11), de 4 de julho de 2024, relativas às transferências de fundos e certas transferências de criptoativos ao abrigo do Regulamento (UE) 2023/1113 ("**Orientações TFR**").

3. Documento referenciados

Esta política deve ser lida em conjunto com a Política de informações que acompanham transferências de fundos e criptoativos.

4. Informação pré-contratual

Previamente à prestação do serviço de transferência, o Banco deverá sempre disponibilizar aos seus clientes todas as informações relacionadas com os serviços de transferência.

As informações deverão ser prestadas em suporte duradouro através do documento de informação pré-contratual, o qual inclui, pelo menos, o seguinte:

- A firma, o endereço da sede e qualquer outro endereço e meio de comunicação, incluindo endereço de correio eletrónico, relevante para as comunicações com o Banco;
- O nome da autoridade competente responsável pela supervisão do Banco;
- Uma descrição das principais características do serviço de transferência a ser prestado;
- Uma descrição da forma e do procedimento para iniciar ou autorizar a transferência e revogar uma ordem ou a autorização, incluindo a especificação das informações que o cliente deve fornecer para que a transferência de criptoativos seja devidamente iniciada ou executada (incluindo como proceder à autenticação);

- As condições com base nas quais o Banco pode rejeitar uma ordem para realizar a transferência;
- O procedimento ou processo estabelecido pelo Banco para determinar o momento de receção de ordens ou da autorização para a transferência, bem como qualquer prazo limite estabelecido pelo Banco para a sua receção;
- Uma explicação, para cada criptoativo, da rede DLT suportada para a transferência desse criptoativo;
- O prazo máximo de execução do serviço de transferência a prestar;
- Para cada rede DLT, o tempo ou o número de confirmações de blocos necessário para que a transferência seja irreversível na rede DLT (ou considerada suficientemente irreversível, no caso de liquidação probabilística), tendo em conta as regras e circunstâncias da rede DLT;
- Todos os custos, encargos ou comissões a pagar pelo cliente ao Banco relativamente ao serviço de transferência, incluindo os relacionados com a forma e a frequência da prestação ou disponibilização de informação e, quando aplicável, a descrição dos montantes desses custos;
- Os meios de comunicação, incluindo os requisitos técnicos para o equipamento e *software* do cliente, acordados entre as partes para a transmissão de informações ou notificações relativas ao serviço de transferência;
- A forma e a frequência com que a informação relacionada com o serviço de transferência será prestada ou disponibilizada;
- As línguas em que o contrato com o cliente será celebrado e em que a comunicação entre as partes será realizada;
- O procedimento seguro para notificação ao cliente, pelo Banco, no caso de suspeita ou ocorrência de fraude ou de incidentes de segurança;
- Os meios e o prazo dentro dos quais o cliente deverá notificar o Banco sobre quaisquer transferências não autorizadas ou incorretamente iniciadas ou executadas, bem como a responsabilidade do Banco, incluindo o montante máximo dessa responsabilidade, por transferências não autorizadas ou incorretamente iniciadas ou executadas; e
- O direito do cliente a cessar o contrato e as formas para o fazer.

As informações contidas no documento de informação pré-contratual devem sempre ser descritas em linguagem facilmente compreensível e de forma clara e acessível.

Mediante pedido do cliente em qualquer momento durante a relação contratual e num prazo razoável, o Banco deverá disponibilizar ao cliente o documento de informações pré-contratuais, de forma gratuita e em suporte duradouro.

Em caso de alteração do documento de informações pré-contratuais, o Banco deverá informar o cliente das alterações com uma antecedência de [2 meses] face à data de entrada em vigor das mesmas.

5. Termos e condições gerais dos serviços de transferência de criptoativos

Previamente à prestação de serviços de transferência de criptoativos e após receber o documento de informações pré-contratuais, o cliente deverá ter aceitado os termos e condições da prestação do serviço de transferência de criptoativos do Banco, os quais incluem, pelo menos, os seguintes elementos:

- A identidade do cliente;
- Os deveres e responsabilidades do cliente e do Banco;
- Uma descrição das modalidades do serviço de transferência prestado;
- Uma descrição dos sistemas de segurança utilizados pelo Banco;
- As comissões cobradas pelo Banco, através de remissão para o preçário do Banco; e
- A lei aplicável.

Mediante pedido do cliente em qualquer momento durante a relação contratual e num prazo razoável, o Banco deverá disponibilizar ao cliente os termos e condições aplicáveis à relação contratual com o cliente, de forma gratuita e em suporte duradouro.

Em caso de alteração aos termos e condições aplicáveis, o Banco deverá informar o cliente das alterações com uma antecedência de [2 meses] face à data de entrada em vigor das mesmas, podendo o cliente, imediatamente e sem encargos, resolver a relação contratual antes da data proposta para a aplicação das alterações.

6. Informação relativa a transferências

Aquando da receção de uma ordem de transferência, mas antes da sua execução, o Banco deverá prestar ao cliente, pelo menos, as seguintes informações:

- Um aviso breve e padronizado sobre se e quando a transferência de criptoativos será irreversível (ou suficientemente irreversível no caso de liquidação probabilística);

- O montante de quaisquer custos relativos à transferência a pagar pelo cliente e, quando aplicável, a discriminação dos valores desses custos.

Esta informação deverá ser prestada ao cliente em suporte duradouro através de meio eletrónico (*homebanking*) e, quando não seja prestada de forma mais frequente que uma vez por mês, gratuitamente. Nos demais casos, o Banco cobrará a comissão prevista no preçário.

O Banco disponibiliza aos clientes, no momento da realização de cada operação de transferência de criptoativos, informação relativa às políticas, procedimentos e disposições internas aplicáveis à gestão de falhas operacionais, incidentes de segurança e riscos de cibersegurança associados ao serviço de transferência de criptoativos.

Para o efeito, cada operação inclui uma referência eletrónica (hiperligação) que remete para uma página dedicada do Banco, onde esta disponível, de forma clara, acessível e permanentemente atualizada, a informação relevante sobre os mecanismos de segurança implementados, procedimentos de reporte e tratamento de incidentes, medidas de mitigação de risco, contactos de suporte e demais disposições aplicáveis ao serviço.

Após a execução de cada transferência, o Banco presta ao cliente pelo menos as seguintes informações:

- Os nomes do ordenante e do beneficiário;
- O endereço da *wallet* na DLT do ordenante ou o número da conta de criptoativos;
- O endereço da *wallet* na DLT do beneficiário ou o número da conta de criptoativos;
- Uma referência que permita ao cliente identificar a transferência;
- O montante e o tipo de criptoativos transferidos ou recebidos;
- A data-valor do débito ou a data-valor do crédito da transferência;
- O montante de quaisquer custos, encargos ou comissões relacionados com a transferência e, quando aplicável, a discriminação dos valores desses custos.

No caso de uma transferência ser rejeitada, devolvida ou suspensa, o Banco deverá informar o cliente, pelo menos, dos seguintes elementos:

- A razão para a rejeição, devolução ou suspensão;
- Se aplicável, como corrigir a situação que originou a rejeição, devolução ou suspensão;
- O montante de quaisquer custos ou encargos suportados pelo cliente e se são reembolsáveis.

7. Receção de ordens, prazos-limite para receção de ordens, prazos de execução e irreversibilidade das transferências

a) Receção de ordens

O cliente pode dar ordens de transferência de criptoativos da sua conta junto do Banco para outras contas de criptoativos junto do Banco, de outros prestadores de serviços de criptoativos ou de carteiras sem custódia (em cumprimento do disposto na Política de Prevenção de Branqueamento de Capitais e Prevenção do Terrorismo em vigor no Banco em cada momento).

Para efeitos de transmissão ao Banco de ordens de transferência de criptoativos, o cliente poderá utilizar os seguintes meios:

- Através do Bison Mobile, mediante inserção dos códigos de segurança necessários à operação em causa e da autenticação forte, quando aplicável;
- Outros meios legalmente admitidos que venham a ser acordados entre as partes, nomeadamente telefone ou correio eletrónico.

As ordens que sejam transmitidas pelo cliente por algum destes meios serão objeto de registo pelo Banco através de um dos seguintes meios:

- Registo informático, se a ordem for transmitida por via telemática; ou
- Outros registos compatíveis com o meio utilizado, designadamente, registo em suporte fonográfico, quando transmitidas por via telefónica.

Uma ordem de transferência considera-se recebida quando é corretamente recebida pelo Banco, através de um dos meios de transmissão de ordens referidos acima e contenha todos os requisitos necessários para a sua execução, nos termos previstos na presente Política.

As ordens de transferência transmitidas pelo cliente ao Banco deverão ser claras e facilmente percetíveis, sem qualquer tipo de correções ou rasuras. Caso não se verifique este requisito, o Banco confirma junto do cliente o conteúdo de quaisquer ordens por ele transmitidas, não sendo responsável por qualquer atraso provocado pela ambiguidade das mesmas.

Para que sejam válidas, as ordens de transferência não podem estar sujeitas a nenhuma condição e devem conter os seguintes elementos:

- O montante e o tipo de criptoativos a transferir;
- O endereço da *wallet* na DLT do beneficiário ou o número da conta de criptoativos;

- caso estejam disponíveis, o nome do beneficiário e os dados de envio (informação adicional sobre a operação) devem igualmente ser disponibilizados.

O cliente e o Banco podem convencionar que a ordem de transferência se tenha por recebida:

- Numa data determinada;
- Decorrido um certo prazo; ou
- Na data em que o cliente colocar criptoativos à disposição do Banco para execução da ordem de transferência.

As ordens de transferência dadas pelo cliente poderão ser revogadas ou modificadas desde que a revogação ou a modificação cheguem ao poder do Banco antes da execução. A modificação de uma ordem constitui a revogação da ordem anteriormente dada e uma nova ordem.

O cliente é responsável pelo pagamento dos encargos, de qualquer natureza, que se mostrem devidos pela revogação ou modificação de qualquer ordem transmitida pelo cliente ao Banco.

b) Prazos-limite para receção de ordens

As ordens de transferência recebidas ou convencionadas como recebidas, nos termos da subsecção anterior, num dia que não seja um dia útil em Portugal, ou a partir das 16 horas, hora de Lisboa, de um dia útil, são consideradas como tendo sido recebidas no primeiro dia útil seguinte, sendo este o momento da sua receção para todos os efeitos legais e contratuais.

c) Prazo de execução de transferências

O Banco assume como compromisso executar as ordens de transferência com a maior brevidade possível desde a sua receção, com vista a garantir que a menor variação possível de valor entre o momento da receção da ordem de transferência e a sua efetiva execução. No entanto, a execução dos procedimentos internos pelo Banco poderá implicar que a execução não seja executada num hiato temporal curto, pelo que estabeleceu prazos máximo de execução de ordens de transferência.

A execução de quaisquer ordens de transferência depende dos procedimentos de segurança que venham, a qualquer momento, a ser definidos ou solicitados pelo Banco, incluindo, limites às transferências realizadas ou sistemas adicionais de autorização por *passwords* específicas geradas para cada operação.

A execução de ordens de transferência pelo Banco está sujeita à verificação dos requisitos para a sua realização previstos na presente Política. Caso estes estejam verificados, o Banco respeitará os seguintes prazos máximos na execução de ordens de transferência, conforme o que ocorrer primeiro:

- Os criptoativos deverão ser creditados na carteira de criptoativos no próprio dia útil em que a ordem de transferência se considere recebida do ordenante e aprovada pelas áreas internas da organização; ou
- Os criptoativos deverão ser creditados na carteira de criptoativos no próprio dia útil em que a verificação dos requisitos para a execução da ordem de transferência ocorra.

O Banco apenas executa transferência de criptoativos dentro da mesma rede DLT.

Findo o prazo de execução sem que o Banco tenha logrado executar a ordem de transferência por motivos que não lhe sejam imputáveis, a ordem de transferência caducará e o cliente deverá ser informado desse facto e da justificação detalhada para o Banco não ter logrado executar a ordem de transferência dentro do prazo previsto.

Em casos excecionais de dificuldades de execução da transferência por causas não imputáveis ao Banco, como períodos de elevado tráfego da rede DLT ou situações de manutenção técnica dos servidores da rede, e previamente ao término do prazo acima referido, o Banco poderá informar o cliente acerca dessas dificuldades, solicitando-lhe que confirme a prorrogação da alidade da ordem por um período adicional de até 24 horas.

d) Irreversibilidade

O Banco deverá aferir, para cada transferência e com base em cada rede DLT, o número de confirmações de bloco necessárias para que as transferências de criptoativos sejam consideradas irreversíveis (ou suficientemente irreversíveis, no caso de liquidação probabilística).

Para criptoativos relativos a redes DLT que utilizam mecanismos de consenso tradicionais, como o *Proof of Work* (*PoW*) ou *Proof of Stake* (*PoS*), o Banco requer um mínimo de 10 confirmações de bloco para que a transferência seja considerada irreversível. Este número de confirmações poderá ser ajustado em função das especificidades da rede e será previamente comunicado ao cliente.

No caso de redes DLT que utilizem liquidação probabilística, o Banco determinará o número de confirmações necessárias para que a transferência seja considerada suficientemente irreversível, com base em critérios de segurança e mitigação de riscos. Estes critérios serão revistos regularmente para assegurar a máxima proteção contra fraudes ou duplicações de transações. Os clientes serão informados, antes de iniciar qualquer transferência, sobre o número de confirmações de blocos exigido para a irreversibilidade da transação, bem como sobre eventuais variações em função da rede DLT utilizada.

Todas as informações relacionadas com os prazos-limite de receção de ordens, prazos de execução de transferências e número de confirmações de blocos necessárias serão disponibilizadas de forma clara e acessível ao cliente, antes da execução de qualquer transferência de criptoativos.

8. Execução, rejeição, devolução ou suspensão de ordens de transferência

Após receção de uma ordem de transferência, o Banco deverá analisar e determinar, caso a caso, de forma justificada e documentada, se a transferência deve ser (a) executada, (b) rejeitada, (c) devolvida ou (d) suspensa.

a) Execução de ordem de transferência

Na ausência de ordens específicas ou no caso de receção de ordens contraditórias de quaisquer pessoas autorizadas a movimentar a conta de criptoativos do cliente, o Banco apenas cumprirá a ordem que primeiro recebeu em condições de ser cumprida ou, em alternativa, poderá recusar o cumprimento dessas ordens sem a sua confirmação por todos os titulares da conta de criptoativos designados para o efeito.

A ordem de transferência de um cliente considera-se cumprida pelo Banco no momento em que o montante de criptoativo objeto da transferência seja depositado na carteira de criptoativos do destinatário junto de uma entidade terceira ou sem guarda, consoante o caso. Para este efeito, o Banco confirma o depósito do montante de criptoativo através de correio eletrónico ou mensagem segura através do Bison Mobile.

O cumprimento das ordens recebidas pressupõe a existência dos criptoativos objeto da ordem, bem como o eventual bloqueio do montante de criptoativos necessários à execução das referidas ordens e ao pagamento de todas as despesas a que haja lugar.

Serão deduzidos ao montante da referida ordem de transferência quaisquer valores que sejam devidos o Banco ou a terceiros por essa transferência, incluindo, sem limitar, as taxas de transação de rede DLT (*gas fees*), sendo tais valores devidamente discriminados na informação a remeter pelo Banco ao cliente nos termos da secção 5 da Política.

O Banco não é obrigada a confirmar o endereço da *wallet* na DLT do beneficiário ou o número da conta de criptoativos fornecido pelo cliente, limitando-se a executar a ordem de transferência com base na informação fornecida pelo cliente.

b) Suspensão da ordem transferência

Quando se verifique alguma das situações previstas na alínea c) da presente secção, e antes de proceder à rejeição da transferência, o Banco deverá suspender a execução da operação de transferência (i.e., não a executar) até à prestação das informações em falta ou à resolução da situação que impossibilita a realização da transferência, quando esta seja possível.

Com exceção dos casos em que tal não seja possível, o Banco deve informar de imediato o cliente da suspensão da operação e solicitar a prestação da informação necessária para dar seguimento à operação, dentro do prazo concedido para o efeito.

Caso não seja possível prosseguir com a execução e o Banco deva rejeitar a operação de transferência, aplica-se o previsto na alínea c) da presente secção.

c) Rejeição de ordem de transferência

Sempre que estiverem reunidos os requisitos previstos na presente Política, o Banco não poderá recusar a execução de uma ordem de transferência autorizada pelo cliente, na qualidade de ordenante, exceto se essa ordem deva ser rejeitada nos termos previstos na Política de Prevenção de Branqueamento de Capitais ou Financiamento do Terrorismo do Banco em vigor em cada momento ou na demais legislação ou regulamentação aplicável.

Quando se verifique uma das situações previstas no parágrafo seguinte, o Banco suspende a operação de transferência antes de a rejeitar. O Banco apenas pode rejeitar uma ordem de transferência quando, após comunicar ao cliente a sua suspensão e, sendo esta passível de resolução, esta não ocorrer dentro do prazo definido para o efeito.

O Banco pode rejeitar uma ordem de transferência quando se verifique uma das seguintes situações:

- Existam dúvidas quanto à ordem recebida ou esta não mostre ser clara ou precisa;
- Se o Banco tiver fundadas dúvidas sobre a identidade do ordenante ou sobre a natureza da operação solicitada;
- Se o ordenante não prestar a informação necessária prevista na Política de Prevenção de Branqueamento de Capitais ou Financiamento do Terrorismo do Banco em vigor em cada momento, no TFR II ou nas Orientações TFR dentro dos prazos aí previstos;
- A ordem de transferência remetida pelo cliente está incompleta ou incorreta e este não disponibiliza as informações em falta ou corrigidas dentro do prazo solicitado;
- O cliente não disponha dos criptoativos que pretende transferir;
- Não estejam cumpridos os requisitos definidos quanto à autenticação necessária para a execução da operação;
- O Banco considere que a realização da operação em questão seja contrária à lei ou possa dar origem a responsabilidade criminal, contraordenacional ou civil do Banco ou de qualquer um dos seus membros dos órgãos sociais ou colaboradores;
- Avaria técnica na rede DLT utilizada para a transferência.

Caso o Banco recuse a ordem de transferência dada pelo cliente, por não se encontrarem reunidas as referidas condições, deverá notificar de imediato o cliente dessa recusa e, se possível, fundamentar a sua decisão, indicando também o procedimento a seguir para a sua correta execução, caso esta seja ainda possível ou admissível.

Na ausência de ordens específicas ou no caso de receção de ordens contraditórias de quaisquer pessoas autorizadas a movimentar a conta de criptoativos do cliente, o Banco apenas cumprirá a ordem que primeiro recebeu em condições de ser cumprida ou, em alternativa, poderá recusar o cumprimento dessas ordens sem a sua confirmação por todos os titulares da conta.

Se a recusa do Banco for objetivamente justificada, poderão ser cobrados ao cliente os encargos inerentes à referida notificação.

Uma ordem de transferência cuja execução tenha sido recusada pelo Banco é considerada como não recebida por esta.

d) Devolução de transferência

Após ter tomado conhecimento da realização de uma operação de transferência não autorizada ou incorretamente executada, o cliente deverá, sem atraso injustificado e dentro do prazo máximo

de 3 (três) meses, tratando-se de consumidor ou microempresa, ou, nos restantes casos, de 2 (dois) meses a contar do respetivo débito, solicitar ao Banco a retificação do movimento.

Apresentada a solicitação pelo cliente, o Banco deve reembolsar prontamente o cliente do montante das operações de transferência que se confirme não terem sido autorizadas por este, e cuja execução ou responsabilidade seja imputável ao Banco.

Nos casos em que essa devolução seja possível, o Banco procede à devolução da transferência de criptoativos quando a transferência tenha sido rejeitada pela rede DLT.

A devolução de criptoativos será acompanhada de uma explicação detalhada ao cliente, incluindo:

- Identificação da tipologia, espécie e montante do criptoativo devolvido;
- Qualquer encargo ou taxa associada à devolução;
- Fundamentos para a devolução.

Nos casos em que a transferência de criptoativos seja executada e se torne irreversível e não seja possível proceder à devolução dos criptoativos, o Banco informa de imediato o cliente deste facto e compromete-se a envidar os melhores esforços para entrar em contacto com o titular da carteira de criptoativos (nos casos da carteira sem guarda) ou com a entidade terceira onde a carteira de criptoativos se encontra depositada para a qual foram enviados os criptoativos com o objetivo de assegurar a sua devolução.

Quando deva proceder à devolução, o Banco privilegia a devolução dos criptoativos em tipo, espécie e montante idêntico ao que foi objeto de transferência. Contudo, caso não seja possível proceder com a devolução em termos idênticos, o Banco procede à devolução no valor correspondente do criptoativo, à data da devolução, em euros ou criptofichas de moeda eletrónica de valor equivalente.

Nestes casos, é aplicável à responsabilidade do Banco pela execução de transferências o disposto na secção 8 abaixo.

9. Responsabilidade do Banco

a) Regras gerais de responsabilidade

O Banco compromete-se a garantir que todas as transferências de criptoativos sejam realizadas de acordo com as ordens válidas do cliente e em conformidade com as normas legais e

regulamentares aplicáveis. Qualquer desvio que resulte em uma transferência não autorizada ou incorretamente executada implicará a análise das circunstâncias para determinar a responsabilidade do Banco.

Caso o Banco execute uma ordem de transferência validamente dada pelo cliente e recebida pelo Banco, ou a execute ou transmita de forma defeituosa, o Banco apenas será responsável caso atue de forma dolosa ou com culpa grave.

Se o endereço da *wallet* na DLT do beneficiário ou o número da conta de criptoativos fornecido pelo cliente for incorreto, mesmo que seja prestado qualquer outro elemento de informação, nomeadamente o nome do beneficiário, o Banco não é responsável pela não execução ou pela execução deficiente da operação de transferência.

O Banco não é responsável por quaisquer danos decorrentes da utilização de qualquer sistema de comunicação utilizado para a comunicação de ordens, nomeadamente decorrentes do atraso, perda, não receção, receção truncada, mutilada ou defeituosa, receção parcial, receção em duplicado, viciação, falsificação, desvio e/ou entrega em local ou a pessoa errados de ordens ou outros elementos enviados pelo cliente ou por terceiro, salvo se tais situações se tiverem ficado a dever a dolo ou culpa grave do Banco.

b) Responsabilidade em caso de operação de transferência não autorizada ou incorretamente executada

Considera-se "transferência não autorizada" qualquer transferência de criptoativos que não preencha algum dos seguintes requisitos:

- O cliente consentiu na sua execução;
- O consentimento foi dado previamente à execução da operação, salvo se for acordado entre o cliente e o Banco que o mesmo devesse ser prestado em momento posterior;
- O consentimento é dado na forma acordada entre o cliente e o Banco;
- O consentimento dado à execução da operação de transferência tenha sido retirado e comunicado ao Banco com a antecedência de 8 horas úteis face à execução da operação.

Uma "transferência incorretamente executada" refere-se a qualquer transferência de criptoativos em que:

- O tipo, espécie ou montante do criptoativo transferido difere daquele autorizado pelo cliente;

- O endereço do destinatário da transferência não é o que foi indicado pelo cliente;
- A transferência não foi realizada de acordo com as instruções do cliente.

De modo a assegurar a segurança do cliente no acesso à sua conta de criptoativos, o Banco aplica a autenticação forte do cliente nos casos em que este:

- Acede em linha à sua conta de criptoativos;
- Inicie uma operação de transferência de criptoativos por via eletrónica;
- Realize uma ação, através de um canal remoto, que possa envolver um risco de fraude na transferência de criptoativos ou de outros abusos.

Caso um cliente negue ter autorizado uma operação de transferência executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao Banco fornecer prova de que a operação de transferência foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo Banco.

O cliente obtém do Banco a retificação de uma operação de transferência não autorizada ou incorretamente executada que dê origem a uma reclamação, se comunicar a operação ao Banco logo que dela tenha conhecimento e sem atraso injustificado, e dentro de um prazo nunca superior a 24 horas a contar da data da transferência, exceto caso esta não tenha prestado ao cliente as informações previstas nas secções 3 e 5 desta Política.

O Banco não está obrigada ao reembolso previsto no parágrafo anterior se tiver motivos razoáveis para suspeitar de atuação fraudulenta do cliente e comunicar por escrito esses motivos às autoridades judiciárias nos termos da lei penal e de processo penal. Nestas situações, recai sobre o Banco o ónus de provar que, no âmbito da sua esfera de competência, a operação de transferência foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de transferência de criptoativos por si prestado.

O cliente suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais das seguintes obrigações:

- Utilizar o serviço de transferência de criptoativos de acordo com as condições acordadas com o Banco e nos termos da presente Política; e
- Comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao Banco a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada

das credenciais de acesso à conta de criptoativos do cliente e estas estejam sujeitas a autenticação forte.

No caso de operações de transferência não autorizadas resultantes de perda, de roubo ou da apropriação abusiva das credenciais de acesso à conta de criptoativos do cliente, com quebra da confidencialidade dos dispositivos de segurança personalizados que seja imputável ao cliente, este suporta as perdas relativas a essas operações.

Sempre que haja lugar ao reembolso do cliente, o Banco assegura que a data-valor do crédito dos criptoativos na conta de criptoativos do cliente não é posterior à data em que o montante foi debitado na conta. Neste caso, o Banco repõe a conta de criptoativos debitada na situação em que estaria se a operação de transferência não autorizada não tivesse sido executada.

c) Responsabilidade em caso de operação de transferência autorizada ou corretamente executada

Se uma ordem de transferência for executada em conformidade com a ordem do cliente, incluindo a identificação da carteira de criptoativos do destinatário, considera-se que foi executada corretamente no que diz respeito ao destinatário especificado nas chaves públicas da carteira. Se a identificação da carteira de criptoativos fornecida pelo cliente for incorreta, o Banco não é responsável pela não execução ou pela execução incorreta da operação de transferência.

No entanto, o Banco envida esforços razoáveis para recuperar os criptoativos envolvidos na operação de transferência com a colaboração de quaisquer entidades terceiras envolvidas na transferência. Caso não seja possível a recuperação dos criptoativos, o Banco fornece ao cliente, mediante solicitação por escrito, todas as informações de que disponha, que sejam relevantes para o cliente poder intentar a correspondente ação judicial.

Quando este seja possível, o cliente tem direito ao reembolso de uma operação de transferência de criptoativos autorizada ou corretamente executada caso estejam reunidas as seguintes condições:

- A autorização não especificar o montante exato da operação de transferência no momento em que a autorização foi concedida; e
- O montante da operação de transferência exceder o montante que o cliente poderia razoavelmente esperar com base nos termos do contrato celebrado com o Banco e nas circunstâncias específicas do caso.

O cliente não tem direito ao reembolso da transferência caso:

- O cliente tenha dado o seu consentimento para a execução da operação de transferência diretamente ao Banco;
- A transferência de criptoativos se tenha tornado irreversível e não seja possível proceder ao seu reembolso sem prejuízo para o Banco; e
- O Banco tenha prestado ou disponibilizado ao cliente as informações previstas nas secções 3 e 5 da presente Política dentro dos prazos aí previstos.

d) Gestão de falhas operacionais e riscos de cibersegurança

O Banco dispõe de recursos humanos e tecnológicos especificamente afetos à gestão de falhas operacionais e de riscos de cibersegurança associados ao serviço de transferência de criptoativos, incluindo funções internas de tecnologia, risco e cibersegurança, bem como serviços especializados prestados por terceiros qualificados.

A monitorização contínua dos sistemas e eventos de segurança é assegurada através de mecanismos de deteção, correlação e resposta a incidentes, incluindo serviços de Security Operations Center (SOC), ferramentas de monitorização e análise de eventos de segurança (SIEM), mecanismos automáticos de alerta e processos formais de escalonamento e resposta a incidentes.

O Banco dispõe ainda de procedimentos internos de gestão, classificação, tratamento, comunicação e recuperação de incidentes relacionados com as TIC e cibersegurança, incluindo mecanismos de escalonamento interno e externo, definição de responsabilidades, resposta operacional, análise forense, recuperação e comunicação às autoridades competentes, quando aplicável.

Os procedimentos operacionais e técnicos aplicáveis encontram-se detalhados na norma interna NOR_SSITM_101 – Procedimento de Gestão de Incidentes e Problemas, incluindo as funções responsáveis, mecanismos de monitorização, processos de resposta e escalonamento aplicáveis ao serviço de transferência de criptoativos.

10. Travel Rule

No contexto da prestação de serviços de transferência de criptoativos, em tudo o que respeita à aplicação dos requisitos de informação e elementos identificativos a obter do ordenante e do beneficiário das transferências de criptoativos, o Banco deverá cumprir integralmente as

disposições estabelecidas no TFR II, nas Orientações TFR e na Política de Prevenção de Branqueamento de Capitais e Financiamento de Terrorismo do Banco em vigor a cada momento.

Todas as transferências de criptoativos realizadas pelo Banco devem ser executadas em conformidade com os requisitos legais e regulamentares aplicáveis.

11. Aprovação e revisão

A presente Política foi aprovada pelo Conselho de Administração em 29 de Junho de 2026 com efeitos imediatos a partir da sua publicação. A Política deve ser sujeita a revisões periódicas, pelo menos anuais, a realizar pelo Conselho de Administração.

Contents

Content:

1. Introduction 21
2. Background 21
2.1. Scope and Purpose 21
2.2. Definitions 21
2.3. Legal framework 22
3. Referenced documents 22
4. Pre-contractual information 22
5. General terms and conditions for crypto-asset transfer services 24
6. Information regarding transfers 24
7. Receipt of orders, deadlines for receipt of orders, execution times and the irreversibility of transfers 24
8. Execution, rejection, return or suspension of transfer orders 27
9. The Bank's liability 31
10. Travel Rule 35
11. Approval and review 35

1. Introduction

This policy on crypto-asset transfer services ("Policy") has been approved by the Board of Directors of Bison Bank, S.A. (**"Bison** Bank" or **"the Bank"**) pursuant to and for the purposes of Article 82 of Regulation (EU) No 2023/1114 of the European Parliament and of the Council of 31 May 2023 ("MiCA"), the ESMA Guidelines on crypto-asset transfer services (ESMA35-1872330276-2032, dated 26 February 2025), Regulation (EU) No 2023/1113 of the European Parliament and of the Council of 31 May 2023 (**"TFR** II"), and the EBA Guidelines (EBA/GL/2024/11) of 4 July 2024 on fund transfers and certain crypto-asset transfers under Regulation (EU) 2023/1113 (**"TFR** Guidelines").

This Policy sets out the procedures relating to compliance with the requirements applicable to the Bank, as a crypto-asset service provider offering crypto-asset transfer services on behalf of customers, including customers' rights in the context of such crypto-asset transfer services.

2. Background

2.1. Scope and Purpose

This Policy applies to all crypto-asset transfer services on behalf of clients, as defined in MiCA[3] , i.e. services involving the transfer, on behalf of a natural or legal person, of crypto-assets (EMTs or Other than EMTs or ARTs) from one distributed ledger address or account to another.

For the purposes of this Policy, distributed ledger technology means a technology that enables the operation and use of distributed ledgers ("DLT")[4] .

This Policy applies to the Bank's employees and to the members of the Board of Directors and the Audit Committee.

2.2. Definitions

For the purposes of this Policy, "clients" are deemed to be all natural or legal persons who (i) are current clients, (ii) are potential clients (i.e., in respect of whom the Bank seeks to enter into a contractual relationship), or (iii) have been clients who have already terminated their contractual

[3] Article 3(1)(26) of MiCA.
[4] Article 3(1)(1) of MiCA.

relationship with the Bank , but in respect of whom the Bank remains bound by post-contractual, fiduciary or similar obligations.

2.3. Legal framework

- Regulation (EU) No 2023/1114 of the European Parliament and of the Council of 31 May 2023 ("MiCA")
- ESMA Guidelines on crypto-asset transfer services (ESMA35-1872330276-2032, dated 26 February 2025)
- Regulation (EU) No 2023/1113 of the European Parliament and of the Council of 31 May 2023 (**"TFR** II")
- EBA Guidelines (EBA/GL/2024/11) of 4 July 2024 on fund transfers and certain transfers of crypto-assets under Regulation (EU) 2023/1113 (**"TFR** Guidelines").

3. Referenced documents

This policy should be read in conjunction with the Policy on information accompanying transfers of funds and crypto-assets.

4. Pre-contractual information

Prior to providing the transfer service, the Bank must always provide its customers with all information relating to transfer services.

The information must be provided on a durable medium via the pre-contractual information document, which must include, at a minimum, the following:

- The name, registered office address and any other address and means of communication, including an email address, relevant for communications with the Bank;
- The name of the competent authority responsible for supervising the Bank;
- A description of the main features of the transfer service to be provided;
- A description of the method and procedure for initiating or authorising the transfer and for revoking an order or authorisation, including details of the information the customer must provide in order for the transfer of crypto-assets to be properly initiated or executed (including how to authenticate);
- The conditions under which the Bank may reject an order to carry out the transfer;
- The procedure or process established by the Bank to determine the time of receipt of orders or authorisation for the transfer, as well as any deadline set by the Bank for their receipt;

- An explanation, for each crypto-asset, of the DLT network supported for the transfer of that crypto-asset;
- The maximum timeframe for the execution of the transfer service to be provided;
- For each DLT network, the time or number of block confirmations required for the transfer to be irreversible on the DLT network (or deemed sufficiently irreversible, in the case of probabilistic settlement), considering the rules and circumstances of the DLT network;
- All costs, charges or fees payable by the customer to the Bank in relation to the transfer service, including those relating to the form and frequency of the provision or making available of information and, where applicable, a description of the amounts of such costs;
- The means of communication, including the technical requirements for the customer's equipment and *software*, agreed between the parties for the transmission of information or notifications relating to the transfer service;
- The manner and frequency with which information relating to the transfer service will be provided or made available;
- The languages in which the contract with the customer will be concluded and in which communication between the parties will take place;
- The secure procedure for the Bank to notify the customer in the event of suspected or actual fraud or security incidents;
- The means and timeframe within which the customer must notify the Bank of any unauthorised or incorrectly initiated or executed transfers, as well as the Bank's liability, including the maximum amount of such liability, for unauthorised or incorrectly initiated or executed transfers; and
- The customer's right to terminate the contract and the procedures for doing so.

The information contained in the pre-contractual information document must always be set out in easily understandable language and in a clear and accessible manner.

Upon the customer's request at any time during the contractual relationship and within a reasonable period, the Bank must provide the customer with the pre-contractual information document, free of charge and on a durable medium.

In the event of any changes to the pre-contractual information document, the Bank must inform the customer of the changes [2 months] in advance of the date on which they come into effect.

5. General terms and conditions for crypto-asset transfer services

Prior to the provision of crypto-asset transfer services and after receiving the pre-contractual information document, the customer must have accepted the terms and conditions governing the provision of the Bank's crypto-asset transfer service, which include, at a minimum, the following elements:

- The customer's identity;
- The duties and responsibilities of the customer and the Bank;
- A description of the terms and conditions of the transfer service provided;
- A description of the security systems used by the Bank;
- The fees charged by the Bank, by reference to the Bank's fee schedule; and
- The applicable law.

Upon the customer's request at any time during the contractual relationship and within a reasonable period, the Bank shall provide the customer with the terms and conditions applicable to the contractual relationship with the customer, free of charge and in a durable medium.

In the event of any changes to the applicable terms and conditions, the Bank must inform the customer of the changes [2 months] in advance of the date on which they come into effect; the customer may, immediately and free of charge, terminate the contractual relationship before the proposed date for the changes to take effect.

6. Information regarding transfers

7. Receipt of orders, deadlines for receipt of orders, execution times and the irreversibility of transfers

e) Receipt of orders

The customer may place orders to transfer crypto-assets from their account with the Bank to other crypto-asset accounts held with the Bank, with other crypto-asset service providers or to non-custodial wallets (in accordance with the provisions of the Anti-Money Laundering and Counter-Terrorist Financing Policy in force at the Bank at any given time).

For the purposes of submitting crypto-asset transfer orders to the Bank, the customer may use the following methods:

- Via Bison Mobile, by entering the security codes required for the transaction in question and undergoing strong authentication, where applicable;

- Other legally permitted means that may be agreed between the parties, namely by telephone or email.

Orders submitted by the customer via any of these means will be recorded by the Bank using one of the following methods:

- Electronic record, if the order is transmitted electronically; or
- Other records compatible with the means used, namely a recording on an audio medium, where transmitted by telephone.

A transfer order is deemed to have been received at the moment it is correctly received by the Bank via one of the means of transmitting orders referred to above and contains all the necessary requirements for its execution, in accordance with the terms set out in this Policy.

Transfer orders transmitted by the customer to the Bank must be clear and easily legible, without any corrections or erasures. Should this requirement not be met, the Bank will confirm with the customer the content of any orders transmitted by them and shall not be liable for any delay caused by the ambiguity of such orders.

To be valid, transfer orders must not be subject to any conditions and must contain the following details:

- The amount and type of crypto-assets to be transferred;
- The *wallet* address on the beneficiary's DLT or the crypto-asset account number ;
- where available, the beneficiary's name and remittance details (additional information regarding the transaction) must also be provided.

The customer and the Bank may agree that the transfer order shall be deemed to have been received:

- On a specified date;
- After a certain period has elapsed; or
- On the date on which the customer makes crypto-assets available to the Bank for the execution of the transfer order.

Transfer orders given by the customer may be revoked or amended provided that the revocation or amendment is received by the Bank prior to execution. The amendment of an order constitutes the revocation of the order previously given and a new order.

The customer is liable for the payment of any charges, of whatever nature, that may be due as a result of the revocation or amendment of any order transmitted by the customer to the Bank.

f) Deadlines for receipt of orders

Transfer orders received or deemed to have been received, in accordance with the previous subsection, on a day that is not a business day in Portugal, or after 4.00 pm Lisbon time on a business day, shall be deemed to have been received on the next business day, which shall be deemed the time of receipt for all legal and contractual purposes.

g) Timeframe for executing transfers

The Bank undertakes to execute transfer orders as promptly as possible upon receipt, with a view to ensuring the smallest possible variation in value between the time of receipt of the transfer order and its actual execution. However, the Bank's internal procedures may mean that execution does not take place within a short timeframe; the Bank has therefore established maximum time limits for the execution of transfer orders.

The execution of any transfer orders is subject to the security procedures that may, at any time, be defined or required by the Bank, including limits on transfers made or additional authorisation systems using specific *passwords* generated for each transaction.

The execution of transfer orders by the Bank is subject to verification of the requirements for their execution as set out in this Policy. Where these requirements are met, the Bank will adhere to the following maximum time limits for the execution of transfer orders, whichever occurs first:

- The crypto-assets must be credited to the crypto-asset wallet on the same business day on which the transfer order is deemed to have been received from the payer and approved by the Bank's internal departments; or
- The crypto-assets must be credited to the crypto-asset wallet on the same business day on which the requirements for the execution of the transfer order are verified.

The Bank only executes crypto-asset transfers within the same DLT network.

If the execution deadline expires without the Bank having been able to execute the transfer order for reasons not attributable to it, the transfer order shall lapse and the customer must be informed

of this fact and of the detailed reasons why the Bank was unable to execute the transfer order within the stipulated timeframe.

In exceptional cases where there are difficulties in executing the transfer for reasons not attributable to the Bank, such as periods of high traffic on the DLT network or situations involving technical maintenance of the network's servers, and prior to the expiry of the aforementioned time limit, the Bank may inform the customer of these difficulties, requesting that they confirm the extension of the order's validity for an additional period of up to 24 hours.

h) Irreversibility

The Bank must assess, for each transfer and based on each DLT network, the number of block confirmations required for crypto-asset transfers to be considered irreversible (or sufficiently irreversible, in the case of probabilistic settlement).

For crypto-assets relating to DLT networks that use traditional consensus mechanisms, such as *Proof of Work* (*PoW*) or *Proof of Stake* (*PoS*), the Bank requires a minimum of 10 block confirmations for the transfer to be considered irreversible. This number of confirmations may be adjusted depending on the specific characteristics of the network and will be communicated to the customer in advance.

In the case of DLT networks using probabilistic settlement, the Bank will determine the number of confirmations required for the transfer to be considered sufficiently irreversible, based on security and risk mitigation criteria. These criteria will be reviewed regularly to ensure maximum protection against fraud or duplicate transactions. Customers will be informed, before initiating any transfer, of the number of block confirmations required for the transaction to be irreversible, as well as of any variations depending on the DLT network used.

All information relating to order acceptance deadlines, transfer execution times and the number of block confirmations required will be made available to the customer in a clear and accessible manner before any crypto-asset transfer is executed.

8. Execution, rejection, return or suspension of transfer orders

Upon receipt of a transfer order, the Bank must analyse and determine, on a case-by-case basis, in a justified and documented manner, whether the transfer should be (a) executed, (b) rejected, (c) returned or (d) suspended.

e) Execution of a transfer order

In the absence of specific instructions, or in the event of receiving conflicting instructions from any persons authorised to operate the client's crypto-asset account, the Bank shall only execute the instruction it first received that is capable of being executed; alternatively, it may refuse to execute such instructions unless they are confirmed by all the designated holders of the crypto-asset account.

A client's transfer order is deemed to have been executed by the Bank at the moment the amount of crypto-assets subject to the transfer is deposited into the recipient's crypto-asset wallet held with a third party or in a non-custodial wallet, as the case may be. To this end, the Bank confirms the deposit of the amount of crypto-assets by email or via a secure message through Bison Mobile.

The execution of orders received is subject to the availability of the crypto-assets covered by the order, as well as the possible blocking of the amount of crypto-assets necessary to execute such orders and to pay any applicable charges.

Any amounts due to the Bank or to third parties in respect of such a transfer, including, but not limited to, DLT network transaction fees (*gas fees*), shall be deducted from the amount of the transfer order in question; such amounts shall be duly itemised in the information to be provided by the Bank to the customer in accordance with section 5 of the Policy.

The Bank is under no obligation to verify the beneficiary's DLT *wallet* address or the crypto-asset account number provided by the customer, and shall merely execute the transfer order on the basis of the information provided by the customer.

f) Suspension of the transfer order

Where any of the situations set out in sub-paragraph (c) of this section arise, and before rejecting the transfer, the Bank shall suspend the execution of the transfer transaction (i.e., not execute it) until the missing information is provided or the situation preventing the transfer is resolved, where this is possible.

Except where this is not possible, the Bank must immediately inform the customer of the suspension of the transaction and request the necessary information to proceed with the transaction, within the time limit set for that purpose.

If it is not possible to proceed with the execution and the Bank is required to reject the transfer transaction, the provisions of sub-paragraph (c) of this section shall apply.

g) Rejection of a transfer order

Where the requirements set out in this Policy are met, the Bank may not refuse to execute a transfer order authorised by the customer, acting as the payer, unless such an order must be rejected in accordance with the Bank's Anti-Money Laundering and Counter-Terrorist Financing Policy in force at any given time or any other applicable legislation or regulations.

Where any of the situations set out in the following paragraph arises, the Bank shall suspend the transfer transaction before rejecting it. The Bank may only reject a transfer order once it has notified the customer of the suspension and, where the matter is capable of being resolved, such resolution has not taken place within the time limit set for that purpose.

The Bank may reject a transfer order where any of the following situations arise:

- There are doubts regarding the order received or it is not clear or precise;
- If the Bank has reasonable doubts regarding the identity of the payer or the nature of the requested transaction;
- If the payer fails to provide the necessary information as set out in the Bank's Anti-Money Laundering and Counter-Terrorist Financing Policy in force at any given time, in TFR II or in the TFR Guidelines, within the time limits specified therein;
- The transfer order submitted by the customer is incomplete or incorrect, and the customer fails to provide the missing or corrected information within the requested timeframe;
- The customer does not hold the crypto-assets they wish to transfer;
- The requirements regarding the authentication necessary for the execution of the transaction have not been met;
- The Bank considers that carrying out the transaction in question would be contrary to the law or could give rise to criminal, administrative or civil liability on the part of the Bank or any of its board members or employees;
- A technical fault in the DLT network used for the transfer.

Should the Bank refuse the transfer order given by the customer because the aforementioned conditions are not met, it must immediately notify the customer of such refusal and, where possible, give reasons for its decision, also indicating the procedure to be followed for the correct execution of the transfer, should this still be possible or permissible.

In the absence of specific instructions, or in the event of receiving conflicting instructions from any persons authorised to operate the customer's crypto-asset account, the Bank shall only execute the instruction it first received that can be carried out; alternatively, it may refuse to execute such instructions without confirmation from all account holders.

If the Bank's refusal is objectively justified, the client may be charged the fees associated with such notification.

A transfer order whose execution has been refused by the Bank is deemed not to have been received by the Bank.

h) Return of a transfer

Upon becoming aware of an unauthorised or incorrectly executed transfer transaction, the customer must, without undue delay and within a maximum period of 3 (three) months in the case of a consumer or micro-enterprise, or, in all other cases, within 2 (two) months from the date of the respective debit, request that the Bank rectify the transaction.

Once the customer has submitted the request, the Bank must promptly reimburse the customer for the amount of any transfer transactions confirmed not to have been authorised by the customer, and for which the Bank is responsible or liable.

Where such a refund is possible, the Bank shall refund the crypto-asset transfer where the transfer has been rejected by the DLT network.

The return of crypto-assets will be accompanied by a detailed explanation to the client, including:

- Identification of the type, class and amount of the crypto-asset returned;
- Any charges or fees associated with the return;
- The grounds for the return.

In cases where the transfer of crypto-assets has been executed and has become irreversible, and it is not possible to return the crypto-assets, the Bank shall immediately inform the customer of this fact and undertakes to use its best endeavours to contact the holder of the crypto-asset wallet (in the case of a non-custodial wallet) or the third party with whom the crypto-asset wallet is held to which the crypto-assets were sent, with the aim of ensuring their return.

Where a return is required, the Bank shall, as a matter of priority, return the crypto-assets of the same type, kind and amount as those transferred. However, if it is not possible to effect the return on identical terms, the Bank shall return the corresponding value of the crypto-asset, as at the date of return, in euros or electronic money tokens of equivalent value.

In such cases, the provisions of section 8 below shall apply to the Bank's liability for the execution of transfers.

9. The Bank's liability

e) General rules on liability

The Bank undertakes to ensure that all transfers of crypto-assets are carried out in accordance with the client's valid instructions and in compliance with the applicable legal and regulatory requirements. Any deviation resulting in an unauthorised or incorrectly executed transfer will entail an analysis of the circumstances to determine the Bank's liability.

Where the Bank executes a transfer order validly given by the customer and received by the Bank, or executes or transmits it in a defective manner, the Bank shall only be liable if it acts with intent or gross negligence.

If the beneficiary's DLT *wallet* address or the crypto-asset account number provided by the customer is incorrect, even if any other information is provided, such as the beneficiary's name, the Bank shall not be liable for the non-execution or defective execution of the transfer transaction.

The Bank shall not be liable for any damages arising from the use of any communication system used for the transmission of orders, in particular those arising from delay, loss, non-receipt, truncated, mutilated or defective receipt, partial receipt, duplicate receipt, corruption, falsification, misdirection and/or delivery to the wrong location or person of orders or other information sent by the customer or a third party, unless such situations are attributable to the Bank's wilful misconduct or gross negligence.

f) Liability in the event of an unauthorised or incorrectly executed transfer

An 'unauthorised transfer' is defined as any transfer of crypto-assets that does not meet any of the following requirements:

- The customer has consented to its execution;

- Consent was given prior to the execution of the transaction, unless it was agreed between the customer and the Bank that consent should be given at a later time;
- Consent is given in the manner agreed between the customer and the Bank;
- Consent given for the execution of the transfer transaction has been withdrawn and communicated to the Bank at least 8 working hours prior to the execution of the transaction.

An 'incorrectly executed transfer' refers to any transfer of crypto-assets in which:

- The type, class or amount of the crypto-asset transferred differs from that authorised by the customer;
- The recipient's address for the transfer is not the one provided by the client;
- The transfer was not carried out in accordance with the customer's instructions.

In order to ensure the customer's security when accessing their crypto-asset account, the Bank applies strong customer authentication in cases where the customer:

- Accesses their crypto-asset account online;
- Initiates a crypto-asset transfer electronically;
- Carries out an action, via a remote channel, which may involve a risk of fraud in the transfer of crypto-assets or other abuses.

Should a customer deny having authorised a transfer transaction that has been executed, or claim that the transaction was not carried out correctly, it is incumbent upon the Bank to provide evidence that the transfer transaction was authenticated, duly recorded and accounted for, and that it was not affected by a technical fault or any other deficiency in the service provided by the Bank.

The customer shall be entitled to have the Bank rectify an unauthorised or incorrectly executed transfer transaction giving rise to a complaint, provided they report the transaction to the Bank as soon as they become aware of it and without undue delay, and within a period not exceeding 24 hours from the date of the transfer, unless the Bank has failed to provide the customer with the information set out in sections 3 and 5 of this Policy.

The Bank is not obliged to make the refund provided for in the preceding paragraph if it has reasonable grounds to suspect fraudulent conduct on the part of the customer and communicates those grounds in writing to the judicial authorities in accordance with criminal law and criminal procedure. In such situations, the burden of proof lies with the Bank to demonstrate that, within the scope of its competence, the transfer transaction was authenticated and duly recorded, and

was not affected by any technical fault or other deficiency relating to the crypto-asset transfer service it provides.

The customer shall bear all losses resulting from unauthorised payment transactions, if such losses are due to fraudulent conduct or the deliberate failure to comply with one or more of the following obligations:

- To use the crypto-asset transfer service in accordance with the terms agreed with the Bank and in accordance with this Policy; and
- To notify the Bank, as soon as the customer becomes aware of the facts and without undue delay, of any loss, theft, misappropriation or unauthorised use of the access credentials to the customer's crypto-asset account, where such credentials are subject to strong authentication.

In the event of unauthorised transfer transactions resulting from the loss, theft or misappropriation of the access credentials to the client's crypto-asset account, where a breach of the confidentiality of the personalised security measures is attributable to the client, the client shall bear the losses relating to such transactions.

Where the client is entitled to a refund, the Bank ensures that the value date for the crediting of the crypto-assets to the client's crypto-asset account is no later than the date on which the amount was debited from the account. In this case, the Bank restores the debited crypto-asset account to the state it would have been in had the unauthorised transfer transaction not been executed.

g) Liability in the case of an authorised or correctly executed transfer transaction

If a transfer order is executed in accordance with the customer's instructions, including the identification of the recipient's crypto-asset wallet, it is deemed to have been correctly executed with regard to the recipient specified in the wallet's public keys. If the identification of the crypto-asset wallet provided by the customer is incorrect, the Bank shall not be liable for the non-execution or incorrect execution of the transfer transaction.

However, the Bank shall use reasonable endeavours to recover the crypto-assets involved in the transfer transaction, with the cooperation of any third parties involved in the transfer. Should it not be possible to recover the crypto-assets, the Bank shall provide the customer, upon written

request, with all information at its disposal that is relevant for the customer to bring the corresponding legal action.

Where possible, the customer is entitled to a refund for an authorised or correctly executed crypto-asset transfer transaction provided that the following conditions are met:

- The authorisation does not specify the exact amount of the transfer transaction at the time the authorisation was granted; and
- The amount of the transfer transaction exceeds the amount the customer could reasonably expect based on the terms of the contract entered into with the Bank and the specific circumstances of the case.

The customer is not entitled to a refund of the transfer if:

- The customer has given their consent to the execution of the transfer transaction directly to the Bank;
- The transfer of crypto-assets has become irreversible and it is not possible to refund it without causing loss to the Bank; and
- The Bank has provided or made available to the customer the information set out in sections 3 and 5 of this Policy within the time limits specified therein.

h) Management of operational failures and cybersecurity risks

The Bank has human and technological resources specifically dedicated to the management of operational failures and cybersecurity risks associated with the crypto-asset transfer service, including internal technology, risk and cybersecurity functions, as well as specialised services provided by qualified third parties.

Continuous monitoring of systems and security events is ensured through mechanisms for incident detection, correlation and response, including Security Operations Centre (SOC) services, security information and event management (SIEM) tools, automated alert mechanisms and formal incident escalation and response processes.

The Bank also has internal procedures for the management, classification, handling, reporting and recovery from incidents relating to ICT and cybersecurity, including internal and external escalation mechanisms, the definition of responsibilities, operational response, forensic analysis, recovery and reporting to the competent authorities, where applicable.

The applicable operational and technical procedures are set out in detail in internal policy NOR_SSITM_101 – Incident and Problem Management Procedure, including the responsible functions, monitoring mechanisms, and response and escalation processes applicable to the crypto-asset transfer service.

10. Travel Rule

In the context of providing crypto-asset transfer services, with regard to the application of the requirements concerning the information and identifying details to be obtained from the payer and the payee of crypto-asset transfers, the Bank must fully comply with the provisions set out in TFR II, the TFR Guidelines and the Bank's Anti-Money Laundering and Counter-Terrorist Financing Policy in force at any given time.

All crypto-asset transfers carried out by the Bank must be executed in accordance with the applicable legal and regulatory requirements.

11. Approval and review

This Policy was approved by the Board of Directors on June 29, 2026 and comes into effect immediately upon its publication. The Policy shall be subject to periodic reviews, at least annually, to be carried out by the Board of Directors.