European Banking Authority

REPORT ON VIRTUAL IBANs

EBA/Rep/2024/08 May 2024

Contents

Executive Summary

In 2023/2024, the EBA carried out a fact-finding exercise on the issuance and use by payment service providers (PSPs) of 'virtual IBANs' (vIBANs). This report summarises the EBA's observations and findings from this fact-finding exercise. It highlights risks and challenges that vIBANs may present to consumers, financial institutions, national competent authorities (NCAs) and to the integrity of the overall EU financial system, based on the six most common vIBAN use cases in the EU.

The report recognises the current absence of a definition of vIBANs and therefore sets out some common characteristics that the EBA has observed, including that vIBANs have the same functionality and format as standard IBANs, which makes them indistinguishable by third parties from standard IBANs, but that vIBANs are linked to a payment account, known as a master account that has its own IBAN, which is different from a vIBAN.

Although the use of vIBANs may present some benefits for consumers, the EBA identified 10 key risks and challenges arising for financial institutions, NCAs and users of vIBANs associated with vIBANs. Some examples of these risks include:

- an unlevel playing field and regulatory arbitrage issues due to divergent interpretations of the applicable legislation by NCAs in different Member States (MS). For example, NCAs have different views on whether the provision of a vIBAN with another MS's country code requires the establishment of a branch in that MS and whether an IBAN (as defined in the Single Euro Payments Area (SEPA) Regulation) always has to be matched 1:1 to a payment account.

- Money laundering / terrorist financing (ML/TF) risk as the end users of vIBANs may be unknown to PSPs, including counterpart PSPs, which means that the information used to monitor transactions may not be reliable; and the lack of visibility for NCAs of the scale of vIBAN offerings in their jurisdiction preventing the NCAs from assessing the adequacy of controls implemented by PSPs to mitigate risks arising from vIBANs.

- Risks to end users of vIBANs arising in circumstances where they are not holders of the master account. In such cases, they may not have a payment account, within the meaning of PSD2, and therefore they may not benefit from all the safeguards and rights in PSD2 associated with having a payment account.

- Consumer detriment due to the lack of transparency of certain key information on e.g. the applicable complaints procedures or the deposit guarantee scheme (DGS) under which the consumer is covered.

The report offers some suggestions about the actions that could be taken by PSPs, the co-legislators and NCAs to mitigate the risks identified in this report. To help PSPs and NCAs identify ML/TF risks in particular, an annex to the report contains a list of risk factors.

1. Background and methodology

1.1 Background

1. In July 2023, the EBA published its Opinion on money laundering and terrorist financing risks[1], which highlighted inter alia the issuance by PSPs of what is commonly referred to as 'virtual IBANs' (vIBANs). The Opinion stated that the use of vIBANs may present risks of ML/TF linked to the lack of legal certainty about the application of customer due diligence (CDD) rules and challenges in respect of transaction monitoring and reporting of suspicious transactions.

2. After publication of the Opinion, the EBA carried out a wider assessment of practices where PSPs or other entities issue or offer vIBANs, looking in particular at the implications from a market integrity, consumer and payments perspective. This report sets out the main characteristics and use cases of vIBANs that the EBA has observed, followed by an identification of the potential benefits of vIBANs, as perceived by market participants, and the risks associated with vIBANs.

3. The report offers suggestions on the actions that could be taken to mitigate the risks identified, including, where necessary, potential changes in Level-1 legislation. While the EBA has identified various use cases in this report, the legitimacy of different business models adopted by PSPs for the vIBANs offering should be assessed on a case-by-case basis, before their implementation, in cooperation with competent NCAs in the MS.

4. The EBA's competence for this work is set out in Articles 8, 9, and 9a of Regulation (EU) 1093/2010 (EBA Founding Regulation), which requires the EBA inter alia to monitor and assess market developments, monitor new and existing financial activities and contribute to protecting the EU's financial system against money laundering and terrorist financing.

1.2 Methodology

5. To inform its assessment, the EBA drew on the following information sources:

   - a survey of NCAs on vIBANs use cases in their jurisdiction, on how financial institutions offering vIBANs are supervised, on risks that the use of vIBANs may present in terms of prudential supervision, consumer detriment, ML/TF and deposit protection, and on the adequacy and effectiveness of controls implemented by PSPs to tackle such risks;

   - interviews with NCAs on specific business models involving vIBANs;

[1] Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector (EBA/Op/2023/08).

- the EBA's prior work on this topic, such as the 2023 Opinion on ML/TF risks[2] and the EBA's Report on ML/TF risks associated with payment institutions (PI)[3];

- a consultation with the industry through bilateral interviews and round-table discussions with more than 20 PSPs, including credit institutions, PI and electronic money institutions (EMIs); and

- information received from the European Commission and Europol.

[2] Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector (EBA/Op/2023/08).

[3] EBA's Report on ML/TF risks associated with payment institutions (EBA/REP/2023/18).

2. Characteristics, use cases, and potential benefits of virtual IBANs

2.1 Characteristics

6. There is currently no legal definition of vIBANs at EU level, and no uniform understanding across NCAs and the industry of what vIBANs are.

7. IBANs are commonly used as payment account identifiers across the EU. More generally, IBANs are mandated in some 60 jurisdictions in the world, with over 20 additional jurisdictions recommending its use for cross-border payments.

8. Article2 (15) of Regulation (EU) No 260/2012 (the SEPA Regulation) defines an IBAN as 'an international payment account number identifier, which unambiguously identifies an individual payment account in a Member State, the elements of which are specified by the International Organisation for Standardisation (ISO)'.

9. The underlying ISO standard 13616-1 (the 'ISO IBAN standard') defines an IBAN, for this standard, as 'an expanded version of the basic bank account number (BBAN), [...] which uniquely identifies an individual account at a specific financial institution, in a particular country'. The ISO IBAN standard describes the elements of an IBAN as a two-letter country code, followed by two check digits and up to 30 alphanumeric characters for a BBAN. According to the ISO IBAN standard:

    - 'the first two letters [of the IBAN] shall always be the two-character country code (alpha-2 code), as defined in ISO 3166-1, of the country in which the financial institution servicing the account resides';

    - the BBAN includes a 'bank identifier', which is defined in ISO IBAN standard as an 'identifier that uniquely identifies the financial institution and, when appropriate, the branch of that financial institution servicing an account'.

10. The forthcoming Regulation on the prevention of the use of the financial system for money laundering or terrorist financing (Anti-Money Laundering Regulation (AMLR)) will include a definition of vIBANs for the anti-money laundering / countering the financing of terrorism (AML/CFT) framework. In the AMLR, a virtual IBAN is defined as 'an identifier causing payments to be redirected to a payment account identified by an IBAN different from that identifier'.

11. Based on the vIBAN use cases the EBA observed, the following characteristics of vIBANs are common to most vIBAN use cases:

- A vIBAN is an identifier that has the same format and functionality as a regular IBAN, and is linked to a payment account, referred to in this report as the 'master account'.

- The master account to which the vIBAN is linked has its own IBAN (different from the vIBAN), and, depending on the use case, can be opened either:

  (a) In the name of the end user of the vIBAN; or

  (b) In the name of another entity which allocates the vIBANs to the end users. For example, in some cases, the master account, with vIBANs linked to it, is opened with a credit institution in the name of the PI or EMI that allocates the vIBANs to its customers (the end users), and also serves as the PI/EMI's safeguarding account for revised Payment Services Directive / E-Money Directive (PSD2/EMD) purposes.

- A vIBAN is used to reroute all incoming payments made towards the vIBAN to the master account, with all incoming payments made towards the vIBAN being credited directly to the master account.

- In some cases, vIBANs can also be used for making payments from the master account towards third parties; in such cases, outgoing payments initiated at the request of the end-user of the vIBAN are debited from the master account.

12. Since all payments made towards a vIBAN are credited directly to the master account, and all payments initiated by the users of vIBANs are made from the master account, vIBANs could be deemed as an identifier of the master account. However, there is no uniform view across NCAs in this regard, with some NCAs taking the view that the vIBANs are an identifier of a separate payment account, different from the master account. This is detailed in Section 3.6 of the report.

13. For third parties, vIBANs are typically indistinguishable from a regular IBAN. For example, where a payment is made by a payer to the user of a vIBAN, the payer's PSP would not be able to discern that the account identifier provided is a vIBAN (instead of a regular IBAN), and will not know the master account to which the funds are transferred.

2.2 Use cases observed

14. vIBANs can serve different purposes and have different functionalities, depending on each use case. For example, vIBANs are often used by companies to automate payment reconciliation. They enable companies to assign individual vIBANs, issued by their PSP, to a specific customer, project, part of a business line, etc. to facilitate the tracking of incoming payments (and, in some cases, also outgoing payments) and reduce the costs associated with payment reconciliation.

15. For example, in some cases, PIs provide to merchants vIBANs that are assigned to each customer of the merchant. This enables the merchant to track and reconcile payments received from its customers, as well as payments made by the merchant to the same account that was used by the merchant's customer to pay in (e.g. refunds, cashing out of an investment). The merchant integrates the PI's systems via application programming interfaces (APIs) and can see all incoming payments made by its customers to the vIBANs, and all outgoing payments made by the merchant to the same account that was used by the merchant's customer to pay in.

16. vIBANs are also used by consumers and companies that wish to have an IBAN with the country code of a given MS, as a way to overcome issues stemming from IBAN discrimination (detailed in Section 2.3).

17. Depending on the use case, vIBANs can enable their users to make and receive payments to or from third parties, or they can be used for a more limited purpose. For example, in some use cases, credit institutions and EMIs provide vIBANs to their customers that can be used by the customers only to top up their e-money account with the credit institution or EMI, or, in the case where the customer requests the redemption of e-money, for the credit institution/EMI to send money to the customer. In such cases, no other incoming or outgoing payments can be made using the vIBANs.

18. vIBAN offerings can be structured in different ways. The EBA identified six use cases through which PSPs, or other entities that partner with a PSP, offer vIBANs to their customers. This list may not be comprehensive and is based on information from NCAs and industry representatives that were interviewed by EBA staff as part of this work.

Use Case 1: PSPs (PIs, EMIs and credit institutions) having a branch in a host MS offer to their customers vIBANs with the country code of that host MS, while the master account is held and serviced from the home MS

19. In some cases, PSPs that have a branch in a host MS offer to their customers vIBANs having the country code of that host MS, while the master account is held and serviced from the home MS.

20. In some of these cases, the branch in the host MS serves mainly to enable the PSP to have access to local payment schemes and to issue vIBANs bearing the country code of that host MS, and the PSP does not carry out other activities via the branch in the host MS, beyond vIBAN issuance (the PSP provides payment services in the host MS based on the freedom to provide services). In other cases, the PSP may also carry out other activities via the branch, such as, for credit institutions, a deposit-taking activity or other activities listed in Annex 1 of the Capital Requirements Directive (CRD), or for PIs and EMIs, the provision of payment and e-money services, as applicable.

Use Case 2: PSPs (PIs, EMIs and credit institutions) partner with another PSP to offer to their customers vIBANs that have been issued by the partner PSP and that include the identifier of the partner PSP and the country code of a host MS in which the partner PSP is authorised or has a branch (without the first PSP having a branch in that host MS)

21. In some MS, PSPs offer to their customers (the 'end users') vIBANs that have been issued by another PSP (the 'partner PSP') that provides the master account and the vIBANs to the first PSP, based on an agreement between these PSPs. In such cases:

    - The vIBANs include the 'bank identifier' (as defined in the ISO IBAN standard)[4] of the partner PSP and the country code of a MS in which the partner PSP is authorised or has a branch.

    - The vIBANs are connected to the master account opened with the partner PSP in the name of the PSP offering the vIBANs to the end users. In some cases, where the latter PSP is a PI or EMI, and the master account is opened with a partner credit institution, the master account may also serve as the PI/EMI's safeguarding account for PSD2/EMD purposes.

    - The partner PSP does not have a contractual relationship with the end users.

22. In some of these cases, the end users of the vIBANs can see through their user interface/app, all incoming and outgoing payments made to/from their vIBANs and are able to share their vIBANs with third parties, showing the vIBAN as their own, as if the vIBAN identified a payment account of the end user. While for the end users, payments appear to be made directly from/to their vIBANs, incoming/outgoing payments are in fact credited to / made from the master account held in the name of the PSP that is the master account holder. For third parties making a payment to the end users, or receiving a payment from the end users, the payments appear as if they are sent to / received from the vIBANs.

Use Case 3: PSPs (PIs or EMIs) partner with a credit institution to offer to their customers vIBANs that have been issued by the partner credit institution and that include the identifier of that credit institution and the country code of the MS in which both the PI/EMI and the partner credit institution are authorised

23. This is similar to Use Case 2 above, with the difference that the PI/EMI that offers the vIBANs to its customers is authorised in the same MS as the partner credit institution, and the vIBANs include the country code of that MS.

Use Case 4: Non-EU financial institutions offer to their non-EU customers vIBANs that have been issued by a partner PSP and that include the identifier of the partner PSP and the country code of the MS in which the partner PSP is authorised or has a branch

[4] See paragraph 8 above.

24. In these cases, similarly to Use Cases 2 and 3 described above, the vIBANs include the identifier of the partner PSP and have the country code of the MS in which the partner PSP is authorised or has a branch. The main difference compared to Use Cases 2 and 3 is that the master account holder is a non-EU financial institution that offers the vIBANs to its non-EU customers.

Use Case 5: Non-EU financial institutions offer to their customers worldwide (including to EU customers) vIBANs that have been issued by a partner PSP and that include the identifier of the partner PSP and the country code of the MS in which the partner PSP is authorised or has a branch

25. This is similar to Use Case 4 above, with the difference that the non-EU financial institution (which is the master account holder) offers the vIBANs to its customers worldwide, including to EU customers. These practices are treated as a separate use case in the report, separately from Use Case 4, because they may give rise to specific risks, as explained in Section 3.9 of the report.

Use Case 6: PSPs offering vIBANs to companies managing payments on behalf of other group companies that allocate the vIBANs to other subsidiaries of the group

26. In some cases, vIBANs are used to support centralisation of payments within a group. In said cases:

    - PSPs offer a master account, together with vIBANs linked to it, to a company (non-financial institution) which performs a treasury function within its group and acts based on a legal mandate to manage payments on behalf of the other group companies.

    - The company which is the master account holder allocates these vIBANs to other group companies (the end users of the vIBANs), which can use the vIBANs to receive and make payments from/to third parties.

    - The master account holder is the only one instructing the PSP to carry out transactions from the master account, on behalf of the end users of the vIBANs.

27. The EBA does not take a view on the legitimacy of the Use Cases 1 to 6 described above. Specific risks in relation to these use cases are presented in Section 3 of this report.

2.3 Potential benefits of vIBANs, as perceived by market participants

28. The main potential benefits of vIBANs, as perceived by market participants, include:

    (a) facilitating payment reconciliation;

    (b) offering consumers and businesses an easier way to obtain an IBAN with the country code of a specific MS, to overcome issues stemming from IBAN discrimination;

(c) facilitating centralisation of payments within a group;

(d) reducing the complexity and costs associated with opening and managing separate bank accounts; and

(e) reduced currency conversion fees for sending and receiving payments in more than one currency.

29. About point (b) above, the EBA notes that vIBANs are sometimes perceived by market participants as a way to overcome issues stemming from IBAN discrimination. IBAN discrimination is commonly understood as referring to a situation where a person is not able to make or receive a SEPA credit transfer, or pay via a SEPA direct debit, from their bank account located in another MS, because the payee refuses to accept an IBAN with a country code other than that of the MS in which the payee is based. As a result, consumers and companies may be unable to access services that require payments, such as telecommunications, utilities or public services. The Court of Justice of the European Union case law confirms that IBAN discrimination for a SEPA credit transfer or direct debit is in violation of Article 9(2) of the SEPA Regulation. However, the practice still occurs which suggests that the SEPA Regulation is insufficiently enforced.

30. Furthermore, in relation to Use Cases 2 and 3 described above, according to some vIBAN providers, some PIs and EMIs rely on a partner credit institution to provide to their customers vIBANs issued by the partner credit institution to overcome issues stemming from lack of direct access of PIs and EMIs to designated payment systems under Directive 98/26/EC (the Settlement Finality Directive). Furthermore, in relation to Use Case 2, according to some vIBAN providers, some PSPs (PIs, EMIs or credit institutions) offer vIBANs that are issued by another partner PSP and that include the country code of a host MS in which the partner PSP is authorised or has a branch, because the alternative for the first PSP of opening a branch in the host MS, connecting to local payment systems and providing accounts with its own IBAN would be a more costly and lengthy process.

3. Risks and challenges associated with vIBANs

31. Based on the EBA's analysis, and considering the limited data available, the main risks and challenges arising for financial institutions, NCAs and users of vIBANs associated with vIBANs include:

- Unlevel playing field and regulatory arbitrage issues stemming from divergent interpretations across NCAs of what vIBANs are;
- risks stemming from lack of visibility for NCAs on the scale of vIBAN offerings in their jurisdiction, leading to risks that the adequacy of PSPs' internal controls framework, including from an AML/CFT perspective, may not be adequately assessed;
- risks stemming from lack of visibility for NCAs of the scale of vIBAN offerings in their jurisdiction raising questions about their ability to assess the adequacy of PSPs' AML/CFT internal systems and controls for vIBANs;
- divergent interpretations on the applicable AML/CFT regulatory framework in case of cross-border provision of vIBANs, leading to risks of AML/CFT supervisory gaps, lack of clarity about the reporting of suspicious transactions to the financial intelligence unit (FIU) and challenges associated with the tracing of suspicious transactions involving vIBANs by FIUs and law enforcement;
- Unlevel playing field and regulatory arbitrage issues stemming from divergent interpretations across NCAs about the way in which the SEPA Regulation and the ISO IBAN standard apply to vIBANs;
- risks arising for the end users of vIBANs where they are not the master account holders, and associated unlevel playing field and regulatory arbitrage issues stemming from divergent interpretation across NCAs about the qualification of the relevant payment services in such cases;
- risks of divergent categorisation and reporting of payment transactions by PSPs under PSD2, where the vIBANs and the IBAN of the master account have different country codes;
- risks of unlevel playing field on the application of the service ensuring verification of the payee introduced by Regulation (EU) 2024/886 on instant credit transfers in euro (the

'Instant Payments Regulation')[5], where the payee using a vIBAN is not the master account holder;

- risks of vIBANs being used by non-EU financial institutions or by EU non-PSPs to provide payment services without the required authorisation;
- risk of divergent supervisory practices about the possibility to issue vIBANs, from a CRD perspective;
- risks arising for consumers using vIBANs and for consumers making a payment to a vIBAN, stemming from lack of transparency; and
- risks arising to users of vIBANs stemming from inappropriate disclosure about which DGS protects their deposits, and risks arising to DGSs.

32. Each of these risks and challenges, which may not be the same for all vIBAN use cases, is described in detail below.

3.1 Unlevel playing field and regulatory arbitrage issues stemming from divergent interpretations across NCAs of what vIBANs are

33. The EBA has observed divergent interpretations across NCAs about the features and definition of vIBANs, and also about the definition of an IBAN in the SEPA Regulation and in the ISO IBAN standard[6].

34. In particular, NCAs interpret differently the terms 'unambiguously' identifying a payment account in the definition of IBANs in the SEPA Regulation and the terms 'uniquely' identifying an 'individual account' in the definition of IBANs in the ISO IBAN standard. Some NCAs interpret those provisions as requiring that an IBAN is always matched 1:1 to a payment account, whereas other NCAs interpret those provisions as allowing for multiple IBANs (a 'primary' IBAN and 'secondary' IBAN) to identify the same account. These divergent interpretations across NCAs also lead to divergent interpretations across NCAs as to whether identifiers used to reroute payments to a master account that has its own IBAN, should be treated as vIBANs or as 'secondary' IBANs.

35. Furthermore, as explained in paragraph 12 above, there is no uniform view across NCAs about whether vIBANs identify the master account to which they are linked, or a separate payment account, different from the master account. This aspect is relevant from a PSD2 perspective, as detailed in Section 3.6 below.

[5] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro.

[6] See paragraphs 8 and 9 above.

36. These divergent interpretations across NCAs lead to an unlevel playing field and regulatory arbitrage issues for PSPs and NCAs. The risk could potentially be mitigated if:

    - the definition of IBAN in the SEPA Regulation were to be clarified as to whether an IBAN always has to be matched 1:1 to a payment account, or whether the same payment account can be identified by multiple vIBANs; and

    - the definition of vIBANs in the AMLR were to be clarified as to whether a vIBAN identifies the master account to which it is connected or a separate account.

3.2 Risks stemming from lack of visibility for NCAs of the scale of vIBAN offerings in their jurisdiction raising questions about their ability to assess the adequacy of PSPs' AML/CFT internal systems and controls relating to vIBANs

37. The EBA has observed that there is a lack of visibility for NCAs about the scale of vIBAN offerings in their respective MS. In this regard, some NCAs indicated that they often find out about vIBAN offerings by PSPs authorised in their jurisdiction only during inspections. NCAs also indicated that they are not always aware that vIBANs are offered in their jurisdiction by PSPs authorised abroad, and that the information in the passport notification in relation to vIBAN use cases is often missing, incomplete or no longer up to date.

38. Furthermore, while most NCAs consider that the use of vIBANs presents significant or very significant ML/TF risks, this view was often based on anecdotal evidence rather than a formal assessment of inherent ML/TF risks, such as the National Risk Assessment or sectoral ML/TF risk assessments. What is more, most NCAs had not carried out a specific assessment of controls put in place by their PSPs to mitigate ML/TF risks associated with vIBANs, for example through on-site inspections or off-site reviews. Those that had carried out such an assessment rated controls as poor or very poor, but indicated that their assessment was not based on a representative sample and may not reflect the overall state of AML/CFT controls in the sector.

39. Lack of sufficient oversight of financial services offered in their MS can make NCAs' supervision less effective and may mean that significant risks, including inadequate internal controls in PSPs issuing or using vIBANs, are not identified or addressed.

40. The risk could be mitigated if:

    - NCAs were to determine the extent to which vIBANs are issued or used by PSPs in their jurisdiction, and enhance their understanding of business models used by PSPs to issue or offer vIBANs in their jurisdiction, including by engaging with relevant industry representatives and by cooperating and exchanging information with other AML/CFT and prudential supervisors.

- NCAs in home and host MS would improve cooperation and exchange information, at the time of both, the initial passport notification and as part of the ongoing supervision of the PSPs' activities, where vIBANs are offered on a cross-border basis.

41. Further, NCAs should consider assessing ML/TF risks to which their PSPs are exposed as a result of them issuing or otherwise being exposed to vIBANs, and take the steps to assess the effectiveness of AML/CFT controls in place at PSPs to mitigate the risks associated with vIBANs. Finally, when assessing ML/TF risks associated with vIBANs, NCAs should consider taking into account the risk increasing and risk mitigating factors mentioned in Annex 1. These risk factors should be viewed in conjunction with risk factors set out in the Anti-Money Laundering Directive (AMLD) and the EBA's Guidelines under Articles 17 and 18(4) of AMLD (EBA/GL/2021/02) (the 'ML/TF Risk Factors Guidelines')[7]

3.3 ML/TF risks stemming from lack of visibility of the identity of the end users of the vIBANs and challenges for PSPs in monitoring their business relationships and their customers' transactions

42. vIBANs may give rise to ML/FT risks stemming from:

(a) lack of visibility for the PSP providing the master account and issuing the vIBANs about the identity of the end users, where the vIBANs are offered to the end users by another PSP, such as in Use Cases 2, 3, 4 and 5 and challenges in such cases for the PSPs providing the master account and issuing the vIBANs in monitoring their business relationships and their customers' transactions; and

(b) lack of visibility for the counterpart PSP involved in a funds transfer about the identity of the end users of the vIBANs, where those end users are not the master account holder.

43. For (a), under the AMLD, PSPs are required to perform ongoing monitoring of their business relationships and their customers' transactions to identify whether they may be unusual or suspicious. In practice this monitoring is based on certain thresholds or indicators, such as the geographical location of a customer or certain transaction patterns.

44. Where a master account, with vIBANs linked to it, is provided to a PSP by a partner PSP, and the PSP offers the vIBANs to its own customers (the end users), such as in Use Cases 2, 3, 4 and 5, based on a contract between the two PSPs, there may be no business relationship between the partner PSP and the end users. In such cases, as is the case in 'correspondent relationships', the partner PSP will have no sight of the identity of the end users nor of the due diligence

[7] EBA's Guidelines (EBA/GL/2021/02) under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines').

measures applied to them. It will not have sight of individual transactions and will therefore focus its transaction monitoring efforts on the overall transactions by the PSP. The ML/TF risk arising from this may be further increased in cases where the PSP offering the vIBANs to the end users is based in a jurisdiction outside the EU (Use Cases 4 and 5), as the AML/CFT standards applied by that PSP may be less robust than those set out in the AMLD.

45. Feedback from the industry suggests that some PSPs providing the master account and the vIBANs to another PSP, which then offers the vIBANs to its own customers, have adopted measures to mitigate this risk. These measures include the PSP providing the master account and issuing the vIBANs and requesting sufficient information from the PSP offering the vIBANs to the end users to ensure that it:

    - Has a good understanding of the robustness of AML/CFT systems and controls of the PSP offering the vIBANs to the end users, for example through questionnaires or through on-site visits, on a risk-sensitive basis.

    - Has a good understanding of the type of services provided by the PSP offering the vIBANs to the end users, to be satisfied that the offering of vIBANs is a reasonable service for this type of PSP.

    - Has a sufficient understanding of the nature of the customer base of the PSP offering vIBANs, so that the PSP is able to monitor transactions in a meaningful way. In exceptional, high ML/TF risk cases, or where ML/TF suspicions arise, this may involve the verification of an end user's CDD information.

46. However, these measures have not been adopted by all PSPs. Furthermore, PSPs' failure to adopt appropriate and sufficient measures has resulted in some PSPs losing their licences.

47. Relatedly, the EBA notes that the above risks may be mitigated by provisions in Article 18(2a) the AMLR, which provides that credit and financial institutions servicing the master account should ensure that they can obtain information on end users of vIBANs, even where vIBANs are issued by another credit or financial institution. The legislation requires that 'this information should be obtained without delay and in any case within no more than five working days'.

48. For Use Cases 2, 3, 4 and 5, the EBA understands that these provisions will require the PSP providing the master account and issuing the vIBANs to satisfy itself that the PSP offering the vIBANs to its own customers (the end users) will provide it with information identifying and verifying the end users of the vIBANs upon request. In other words, for Use Cases 2, 3, 4 and 5, the EBA understands the reference to 'the institution issuing the virtual IBAN' as referring to the PSP offering the vIBANs to the end users.

49. For (b), Article 4(1)(b) of Regulation (EU) 2023/1113 (the Funds Transfer Regulation (FTR)) requires the PSPs to provide information on the payer's payment account. The FTR does not

appear to require the PSP to provide the information on the end user in situations described in paragraphs 70 to 72 of this report, where the end user is not a holder of a master account and may not have a payment account. This could mean that the information provided with the fund transfer may be misleading or incomplete. The Financial Action Task Force (FATF) has recognised this risk and is currently consulting on changes to Recommendation 16 in this regard[8].

50. PSPs are responsible for identifying risks associated with their business, including various products and services provided by them, and for putting in place appropriate controls to mitigate these risks. When assessing the effectiveness of the PSPs' controls, NCAs may consider whether the PSPs draw on multiple risk factors when monitoring transactions to ensure that the transaction monitoring system flags apparent discrepancies for further investigation. Guideline 4 of the EBA's ML/TF Risk Factors Guidelines has further information on this point.

51. Further, NCAs could assess on a case-by-case basis the extent to which institutions within their supervisory remit enter into a correspondent relationship with other PSPs in the vIBANs context and communicate their regulatory expectations to the sector accordingly. Guideline 8 of the EBA's ML/TF Risk factors Guidelines contains further information on the risk mitigation measures institutions can put in place.

52. Furthermore, to address the challenges mentioned above about the lack of transparency of the ultimate originator/beneficiary of a payment, it may be necessary to require that PSPs, under the SEPA schemes, include in the payment message remittance information about the end user on whose behalf a payment is made or received. In this regard, the EBA notes that, while the revision to the ISO 20022 standard presents the ability to share information on the 'ultimate' parties in financial transactions – ordering customer (referred to as 'ultimate debtor'), and beneficiary (referred to as 'ultimate creditor'), on a voluntary basis, when processing transfers in the context of 'payments and collections/receivables on behalf of' (POBO & COBO), the sharing of information on the 'ultimate' parties is not mandatory for SEPA Credit Transfers[9].

3.4 Divergent interpretation of applicable AML/CFT regulatory framework for the cross-border provision of vIBANs, leading to risks of AML/CFT supervisory gaps, lack of clarity about FIU reporting and challenges associated with the tracing of

[8] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-public-consultation-Feb24.html.

[9] Existing SEPA schemes offer the possibility to include in the payment message 'Extended Remittance Information' (ERI), which allows PSPs to include within the payment message (i) unstructured remittance information with the Payment Description and (ii) Structured Remittance Information based on the ISO 20022 standard. However, the Extended Remittance Information is not mandatory and does not guarantee end-to-end transmission of 'end user' data.

suspicious transactions involving vIBANs by FIUs and law enforcement

53. There are divergent views across NCAs about the division of AML/CFT supervisory responsibilities between the home and host NCA in cases where the master account is held in a different MS from that of the end customer and where a vIBAN contains a different country code from the IBAN of the master account. These divergent approaches create a risk of supervisory gaps and risks of regulatory arbitrage.

54. Furthermore, some PSPs have raised concerns that it is not always clear to which FIU a suspicious transaction report should be submitted: the FIU of the MS referred to in the country code of the vIBAN and in which the PSP has a branch or the FIU of the MS where the master account is held, and through which transfers are processed. vIBANs can also make the tracing of suspicious transactions by law enforcement more difficult, as they obscure the location of the master account and consequently, the customer's funds.

55. Some MSs have taken steps to clarify expectations in such cases. For example, in one MS, the bank account register also captures holders of vIBANs. AMLD6 will require all national bank account registers to hold information on vIBANs and their holders.

56. At the same time, the FATF is consulting on changes to its Recommendation 16 and is proposing that 'The account number or the associated payment message data should enable the institutions and supervisors to identify the financial institution and the country where the account holder's funds are located'.

57. In line with the principle of territoriality and the provisions in Article 48(4)[10] of the AMLD, NCAs are responsible for the AML/CFT supervision of obliged entities that have an establishment like a branch in their MS. There are, however, divergent views among NCAs whether the sole activity of issuing vIBANs by PSPs warrants the establishment of a branch (refer also to Section 3.10 in this report).

58. Furthermore, due to the specific nature of some vIBAN use cases, there are limited or no activities performed in the branch, but instead the onboarding of customers and transactions are carried out via the head office entity. This means that the host NCA may have only limited sight of transactions or CDD measures applied. Therefore, the EBA highlights that the home NCA is responsible for the supervision of activities carried out via the head office and also the implementation of the group-wide policies and procedures. It is pertinent for the home and host NCAs to cooperate closely and, in line with their respective competencies, ensure that PSPs put in place the necessary systems and controls according to the applicable legislation to monitor transactions made to or from the master account. This also includes in Use Cases 2, 3,

[10] Article 48(4) AMLD requires that 'the competent authorities of the Member State in which the obliged entity operates establishments supervise that those establishments respect the national provisions of that Member State transposing this Directive.'

4 and 5 where the PSP providing the master account and issuing the vIBAN is different from the PSP offering the vIBANs to the end users. Where AML/CFT colleges exist, the coordination of tasks from an AML/CFT perspective between the home and host NCAs could be discussed in that college.

59. Furthermore, the EBA recalls that Article 45 AMLD requires that group-wide policies and procedures should be implemented across the group. Some, but not all, PSPs with which the EBA met confirmed that they adopt the highest AML/CFT standards of all MS in which they operate and implement those in their group-wide policies and procedures. The EBA considers this to be a good practice, however it could not determine how common this approach is across the EU.

3.5 Unlevel playing field and regulatory arbitrage issues stemming from divergent interpretations across NCAs about the way in which the SEPA Regulation and the ISO IBAN standard apply to vIBANs

60. There is no uniform view across NCAs about the way in which the SEPA Regulation and the ISO IBAN standard apply to vIBANs.

61. More specifically, for Use Case 1, while some NCAs allow PSPs with a branch in a host MS to issue vIBANs bearing the country code of a host MS, while the master account is held in the home MS and serviced from there, two NCAs are of the view that this would not be in line with the ISO IBAN standard and the SEPA Regulation. These latter NCAs require PSPs issuing vIBANs with the country code of a host MS, using a branch in the host MS, to ensure that the master account is serviced from the host MS, and not from the home MS. In other words, these NCAs require that there is no divergence between the country code of the vIBAN and the country code of the IBAN of the master account.

62. In support of their view, these latter NCAs refer to the provisions of the ISO IBAN standard which state that:

    - 'the first two letters [of the IBAN] shall always be the two-character country code (alpha-2 code), as defined in ISO 3166-1, of the country in which *the financial institution servicing the account resides'*;

    - the BBAN, which is part of the IBAN structure, includes the 'bank identifier of the financial institution servicing the account'; the 'bank identifier' is defined in the ISO standard as an 'identifier that uniquely identifies the financial institution, *and when appropriate, the branch of that financial institution servicing the account'* [emphasis added].

63. In this regard, the EBA notes that, while views across NCAs on this point diverge, the SEPA Regulation does not explicitly prohibit practices such as those described in Use Case 1, where

PSPs with a branch in a host MS issue vIBANs with the country code of that host MS that are linked to a master account held and serviced from the home MS. Furthermore, in relation to Use Case 1, the EBA understands that, in the European Commission (EC) services' preliminary view:

- the notion of 'residence' of the 'financial institution' referred to in the ISO IBAN standard can be equated with the notion of 'establishment' in EU law for the objectives and purposes of the SEPA Regulation;

- according to the ISO IBAN standard, a PSP can issue IBANs bearing the country code of a host MS, provided that the PSP has an establishment, such as a branch, in that host MS;

- the issuance of local IBANs bearing the country code of a host MS while the master account is held and serviced from the home MS is not against the ISO IBAN standard or the SEPA Regulation.

64. Furthermore, for Use Cases 2, 4 and 5, there is no uniform view across NCAs whether such practices are in line with the SEPA Regulation and the ISO IBAN standard. While some NCAs allow such practices, other NCAs believe that such practices are not compliant with the SEPA Regulation and the ISO IBAN standard.

65. These latter NCAs believe that such practices are not in line with the provisions in the ISO IBAN standard which provide that 'the first two letters [of the IBAN] shall always be the two-character country code […] *of the country in which the financial institution servicing the account resides'* [emphasis added]. In their view, in order for a PSP to offer to its customers (the end users) vIBANs with the country code of a given MS, that PSP should be either authorised or have a branch in that MS, and cannot rely on the fact that the partner PSP (providing the master account and issuing the vIBANs) has a branch or is authorised in that MS, unless there is a contractual relationship between the partner PSP and the end users of the vIBANs.

66. In this regard, the EBA notes that it is unclear how the reference in the ISO IBAN standard to the 'financial institution servicing the account' should be interpreted for vIBANs, and in particular in the context of Use Cases 2, 4 and 5. In the EBA's view, if the vIBAN is deemed as an identifier of the master account, as explained in paragraph 12 above, then the reference in the ISO IBAN standard to the 'financial institution servicing the account' could be interpreted as referring to the PSP providing the master account and issuing the vIBANs. If such an interpretation were to be taken, this would mean that practices where a PSP (e.g. a PI/EMI) offers to its customers vIBANs that have been issued by another partner PSP (e.g. a credit institution) and which bear (i) the bank identifier of the partner PSP; and (ii) the country code of a MS in which the partner PSP is established or has an establishment, would be in line with the ISO IBAN standard.

67. The divergent interpretation across NCAs outlined above about the way in which the SEPA Regulation and the ISO IBAN standard apply to vIBANs create an unlevel playing field and regulatory arbitrage issues.

68. These issues can potentially be mitigated by clarifying, in Level-1 legislation:

- how the SEPA Regulation and the ISO IBAN Standard apply in relation to the vIBANs use cases described above; and

- the legal qualification of the relationship between the PSP offering the vIBANs to the end users and the partner PSP providing the master account and issuing the vIBANs to the first PSP in Use Cases 2, 3, 4 and 5.

3.6 Risks arising for the end users of vIBANs where they are not the master account holder, and associated unlevel playing field and regulatory arbitrage issues stemming from divergent interpretation across NCAs about the qualification of the relevant payment services in such cases

69. As explained in paragraph 12 above, considering that all payments made towards a vIBAN are credited to the master account, and that all payments initiated by the end users of vIBANs are made from the master account, vIBANs could be deemed as an identifier of the master account to which the vIBANs are linked. However, as explained in paragraph 12, there is no uniform view across NCAs in this regard, with some NCAs taking the view that a vIBAN is an identifier of a separate payment account, different from the master account. For example, one NCA is of the view that, where the vIBAN and the master account have different country codes, the vIBAN cannot be deemed as identifying the master account, as that would mean that the account is located in two different countries. In said NCA's view, in such cases, the vIBAN identifies a separate payment account (or 'redirection account') through which funds are channelled to/from the master account. Also, in said NCA's view, the sole fact of keeping a record of the balance of the vIBAN user constitutes the provision of a payment account that is different from the master account, even if all payments are made from/sent to the master account.

70. If the vIBAN is deemed as an identifier of the master account to which it is linked, as explained in paragraph 12 above, then where the end users of the vIBANs are not the holder of the master account, the master account cannot be deemed as the payment account of those end users, since it is held in the name of another person. This is because PSD2 defines a payment

account as 'an account *held in the name of one or more payment service* users which is used for the execution of payment transactions' (Article 4 (12) of PSD2)[11].

71. In such cases, a risk arises that those end users may not have a payment account, within the meaning of PSD2, and therefore they may not benefit from all the safeguards and rights in PSD2 associated with having a payment account (including in terms of disclosure requirements, application of strong customer authentication and access by account information and payment initiation service providers to payment accounts).

72. Where the end users of the vIBANs do not have a payment account, this also has ramifications about the legal qualification of the payment services provided by the respective PSPs to the end users (e.g. as money remittance vs credit transfers). In this regard, while money remittance implies that no payment account is created in the name of the payer[12], a credit transfer implies that funds are transferred from the payer's payment account[13]. This creates a risk of divergent interpretations across NCAs about the qualification of the payment services provided by the PSPs offering the vIBANs to the end users, in the specific case mentioned above, which can lead to an unlevel playing field and regulatory arbitrage issues.

73. The risk could be mitigated by the PSD2 clarifying the definition of a 'payment account' and in particular whether users of vIBANs that are not the holder of the master account holder, such as in Use Cases 2 and 3 above, are considered to have a payment account within the meaning of PSD2.

3.7 Risks of divergent categorisation and reporting of payment transactions by PSPs under PSD2, where the vIBANs and the IBAN of the master account have different country codes

74. Where the vIBANs and the IBAN of the master account have different country codes, the payer's PSP making a payment towards a vIBAN (of the payee) is typically unable to identify whether the payee's account identifier is a vIBAN or a standard IBAN and does not have visibility in which country the master account is held and where funds are transferred.

75. This means that, in such cases, the payer's PSP may not be able to distinguish between domestic vs cross-border payment transactions for reporting under Article 96(6) of PSD2 and the EBA Guidelines on fraud reporting under PSD2. This may lead to divergent categorisation

[11] A payment transaction is defined in PSD2 as 'an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee'.

[12] Money remittance is defined in Article 4(22) of PSD2 as 'a payment service where funds are received from a payer, *without any payment accounts being created in the name of the payer* or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee' [emphasis added].

[13] A credit transfer is defined in Article 4 point (24) of PSD2 as 'a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions *from a payer's payment account* by the payment service provider which holds the payer's payment account, based on an instruction given by the payer' [emphasis added].

and reporting of payment transactions under the EBA Guidelines on fraud reporting under PSD2 and to distorting the data on fraud collected under these Guidelines for domestic and cross-border transactions.

76. To mitigate this risk, PSD2 could clarify how the payer's PSP should report transactions made towards a vIBAN when the vIBAN has a different country code from that of the master account, considering the aspects mentioned above.

3.8 Risks of unlevel playing field in the application of the service ensuring verification of the payee introduced by the Instant Payments Regulation, where the payee using a vIBAN is not the master account holder

77. Article 5c(1) of the SEPA Regulation, as inserted by the Instant Payments Regulation, introduces an obligation for the payer's PSP, for credit transfers in euro, to offer the payer a service ensuring the verification of the name of the payee against the IBAN of the payee provided by the payer. This obligation applies both for instant credit transfers and standard credit transfers.

78. To enable the payer's PSP to perform such checks, Article 5c(1)(a) requires 'the payee's PSP', upon request from the payer's PSP, to verify whether the IBAN and the name of the payee provided by the payer match. According to Article 5c(1):

    (a) Where the name of the payee and IBAN do not match, the payer's PSP is required, based on information provided by the payee's PSP, to notify the payer thereof and inform the payer that authorising the credit transfer might lead to transferring the funds to a payment account not held by the payee indicated by the payer.

    (b) Where the name of the payee and the IBAN almost match, the payer's PSP is required to indicate to the payer the name of the payee associated with the IBAN provided by the payer.

79. Article 5c(1)(c) of the same Regulation further provides that 'where a payment account identified through [an IBAN] provided by the payer is held by a PSP on behalf of multiple payees', '*the PSP maintaining that payment account on behalf of multiple payees or, where appropriate, the PSP holding that payment account*, shall, upon the request of the payer's PSP, confirm whether the payee indicated by the payer is among the multiple payees on whose behalf the payment account is maintained or held [emphasis added]'.

80. The EBA notes that it is unclear how the above requirements for the 'payee's PSP' apply in Use Cases 2 and 3, where:

- a payer wishing to make a credit transfer to a payee that uses a vIBAN provides to its PSP, before the credit transfer is authorised, the name of the payee and the vIBAN of the payee;

- the payee/vIBAN end user is not the holder of the master account (the account is held in the name of the PSP offering the vIBANs to the payee / vIBAN end user);

- the payer's PSP sends to the PSP that provides the master account and that issued the vIBAN the request to verify whether the vIBAN and the name of the payee match;

- the latter PSP does not have a contractual relationship with the payee/the vIBAN end user, and does not know who the end user of the vIBAN is (this could be the case in the interim period before Article 18(2a) of the AMLR applies[14]).

81. In such scenario, it is unclear whether the obligation in Article 5c(1) for 'the payee's PSP' to provide the respective information to the payer's PSP is incumbent on: (a) the PSP that provides the master account and issued the vIBAN; or (b) the PSP that offers the vIBAN to the payee / the vIBAN end user, considering that the former PSP does not have a contractual relationship with the payee / the vIBAN end user. Also, in the scenario described above, it is unclear what response the respective PSP should provide to the payer's PSP, given that the payee / vIBAN end user is not the holder of the master account.

82. To mitigate such risks, further clarifications in Level 1 legislation on how the above provisions in Article 5c(1) of the SEPA Regulation apply in the scenario above would be helpful.

3.9 Risks of vIBANs being used by non-EU financial institutions or by EU non-PSPs to provide payment services without the required authorisation

83. In Use Case 5, where a non-EU financial institution offers to its customers worldwide, including EU customers, vIBANs that have been issued by an EU PSP, there is a risk that the non-EU financial institution may be performing payment or other banking services in the EU without the necessary authorisation under the PSD2 or the CRD. Such risks would need to be assessed on a case-by-case basis to determine whether the non-EU financial is providing payment services within the EU.

84. Similar risks might also arise where a company (non-PSP) that holds a master account with a PSP provides to other users vIBANs that have been issued by the PSP to the first company, enabling those users to make and receive payments to/from third parties. Such cases need to be assessed on a case-by-case basis, i.e. to determine:

[14] Referred to in paragraph 47-48 above.

a) whether the respective payment transactions fall within the scope of PSD2 or are excluded from the scope of the Directive based on an exclusion in Article 3 PSD2; and

b) where the respective payment transactions fall within the scope of PSD2, whether the non-PSP (the master account holder) acts as an agent of the partner PSP.

85. Where the master account holder is providing payment services in the EU without the required authorisation, risks arise for the end users of the vIBANs who may not benefit from the protection offered by PSD2 (including in terms of safeguarding of customer funds, liability for fraudulent transactions, disclosure requirements etc.). Also, this gives rise to unlevel playing field issues for other PSPs operating in the EU.

86. Furthermore, where the master account holder provides payment services without the required authorisation, this can also expose the EU PSP offering the master account and issuing the vIBANs to reputational and possibly legal risks.

87. The risk can be mitigated by NCAs checking, where such use cases exist in their MS that the issuance of vIBANs to a non-EU financial institution or to an EU non-PSP does not result in the unauthorised provision of payment or other banking services in the EU by non-EU financial institutions or by non-PSPs. Where such risks materialise, NCAs should take the necessary supervisory actions.

3.10 Risks of divergent supervisory practices about the possibility to issue vIBANs, from a CRD perspective

88. The main risk identified by the EBA from a CRD perspective for vIBANs relates to the question whether the issuance of vIBANs by a branch meets any activity listed in Annex I CRD.

89. In relation to Use Case 1, based on the findings of the survey conducted with NCAs, there are divergent views across NCAs about the possibility of a credit institution to establish a branch in a host MS for vIBAN issuance while the master account is held and serviced from the home MS.

90. While most NCAs indicated that they have not encountered such a scenario and did not express a policy view, divergent views have been expressed by those NCAs which have come across the practices described in Use Case 1.

91. Notably, a few NCAs indicated that, as host supervisors, they do not allow credit institutions authorised in another MS to establish a branch in their jurisdiction for the sole purpose of issuing vIBANs with the country code of the host MS. In the view of these NCAs, branches of credit institutions should perform at least an activity listed in Annex I to the CRD, and the issuance of vIBANs cannot be considered as a banking activity listed in Annex I to the CRD. Therefore, in their view, a branch set up in the host MS solely for the issuance of vIBANs

bearing the country code of the host MS is not a 'branch' within the meaning of CRD. By contrast, other NCAs believe that credit institutions can establish a branch in a host MS where the activity of that branch is limited only to vIBAN issuance and the master account is held and serviced from the home MS. Divergent approaches have therefore emerged as to the nature of the issuance of vIBAN.

92. Moreover, Use Cases 2 and 3 require additional analysis and supervisory assessment of the arrangements in place. In this context, the EBA advises NCAs of the home and host MS to enquire with their own supervised entities the legal basis for such a partnership arrangement. In relation to Use Case 2, the EBA advises NCAs to enhance their cross-border cooperation and exchange of information in whatever forum available, either passport notifications, supervisory colleges or other settings.

93. It could be clarified, in particular for Use Case 1, to what extent the sole issuance of a vIBAN in a host MS is covered by the CRD passporting provisions through the review of Annex I CRD where needed.

3.11 Risks arising for consumers using vIBANs and for consumers making a payment to a vIBAN, stemming from lack of transparency

94. Some of the risks outlined above, such as risks that users of vIBANs may not benefit from the safeguards in PSD2 when they are not the master account holder, can also impact consumers.

95. In addition, vIBANs can also increase risks for consumers in cases of inappropriate disclosure in the pre-contractual information, which may lead to consumers not understanding the product/service they are contracting, or in cases of inappropriate disclosure in the contractual information for vIBANs.

96. Furthermore, there is also a risk that consumers may not understand to which NCAs they can submit a complaint for cross-border offerings of vIBANs, especially in the scenario where the vIBAN and the IBAN of the master account have different country codes, due to lack of clarity about the allocation of competencies between the NCAs of the host and home MS.

97. vIBANs may also raise risks and challenges for consumers making a payment to a payee which uses a vIBAN. These include:

    - risks that consumers may be misled to think they are paying to an account held in one country (e.g. their own country), which may give more comfort to the consumer, when in fact the funds are transferred to a master account in a different country;

- challenges in the enforcement of consumer claims towards the payee, and in the prosecution of fraudulent activities, especially where the vIBAN and the IBAN of the master account have different country codes;

- lack of clarity for consumers to which NCAs they can submit a complaint especially in the scenario where the vIBAN and the IBAN of the master account have different country codes.

98. The risk could be mitigated by clarifications as to which NCAs consumers are meant to submit a complaint for a cross-border offering of services based on vIBANs business models. Furthermore, NCAs could check that PSPs provide sufficient and comprehensible information to consumers using vIBANs for the vIBANs services offered by PSPs, both at the pre-contractual stage as well as in the contract with the consumer, according to the applicable legal requirements.

3.12 Risks arising to users of vIBANs stemming from inappropriate disclosure about which DGS protects their deposits, and risks arising to deposit guarantee schemes

99. vIBANs may also raise risks and challenges from a deposit protection perspective. In particular, depending on the use case, it may not always be clear to customers which DGS protects their deposits. While there already is some scope for confusion for the customers even where there is no vIBAN and a customer opens an account at a branch of a credit institution headquartered in another MS, the use of vIBANs may complicate the set up even further.

100. This is particularly relevant in Use Case 2, where a branch of a credit institution enters into a partnership arrangement with another credit institution in another MS to offer to the branch's customers vIBANs bearing the identifier of the partner credit institution and the country code where the partner credit institution is established. This may result in a situation where the branch customer's funds are protected neither by the DGS where the branch is located, nor the DGS where the credit institution providing the vIBANs to its customers is headquartered, but the DGS of the partner credit institution.

101. The general lack of transparency and proper disclosure of information at (pre-contractual) stage of terms and conditions applicable to consumers also applies to deposit protection, and can arise even in relation to standard IBANs, but the use of vIBANs amplifies the risk of confusion for the customers. In the EBA Opinion on the eligibility of deposits, coverage level and cooperation between DGSs published in August 2019, the EBA recommended to amend the way depositors are informed about deposit protection upon opening an account and then periodically. The EBA's Recommendation is now reflected in the EU Commission's proposal for the revised deposit guarantee schemes directive (DGSD) and proposes that the EBA should

develop a legal instrument outlining the details of such information, and how it ought to be provided to the depositors.

102. vIBANs may also pose potential issues with traceability of funds in the context of a DGS payout, in particular where the customer's name attached to the vIBAN and the name attached to the master account to which the vIBAN is linked are different. In such a case, it might be that following a bank failure, the depositor provides the DGSs with a vIBAN as the account where the depositor would like to receive their reimbursed funds, without the DGS knowing if the master account belongs to that person.

103. Finally, in instances where customers' funds with a PI/EMI are placed by the PI/EMI in a safeguarding account at a credit institution, such deposits may or may not be protected where the institution holding the client funds fails. That is the case, because, as shown in the EBA Opinion on the treatment of client funds[15] published in October 2021, the approach to protecting client funds differs across the EU. The EBA has recommended to the Commission to amend the DGSD to ensure such client funds are protected, and such an amendment is included in the proposal for the revised DGSD. While this risk is not specific to vIBANs, the use of vIBANs may make the issue more prevalent if customers across the EU were to use vIBANs issued by PI/EMI as opposed to using regular IBANs, and thus the amount of safeguarded deposits were to increase.

104. The risk could potentially be mitigated by NCAs checking that PSPs provide sufficient information to users of vIBANs, both at the pre-contractual stage and in the contract with the customer to ensure that depositors using a vIBAN are made aware which DGS protects their deposit. Furthermore, to mitigate the risk mentioned above on the traceability of funds in the context of a DGS payout, DGSs could ensure, as part of their internal procedures, that depositors claiming their reimbursement provide the DGS with the IBAN where they request to receive the reimbursement, and indicate if the ultimate beneficiary is different from the depositor requesting the transfer.

15 https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2021/1022906/EBA%20Opinion%20on%20the%20treatment%20of%20client%20funds%20under%20DGSD.pdf

Annex 1: ML/TF risks associated with vIBANs – risk indicators

These risk indicators should be considered in conjunction with the relevant risk factors set out in the EBA's Guidelines on ML/TF Risk Factors. The risk indicators listed here are not exhaustive and there is no expectation that all risk factors are considered in all cases.

The risk exposure is higher in those use cases where the following risk indicators are present:

- the lack of a contractual relationship between the PSP servicing the master account and issuing the vIBANs and the end users of vIBANs as this means that the identity or location of the end user may not always be known to the PSP servicing the master account;
- the lack of transparency of end users transactions;
- no limitations applied by a PSP on the number of vIBANs that may be held by one end user;
- a holder of a master account or, if different, an end user of a vIBAN is based in a high risk non-EU country or a country where the AML/CFT rules are less stringent than those set out in the AMLD;
- issuing documents that associate the vIBAN with names of third parties other than the verified account holder of the master account or any feature that causes confusion about the identity of the account holder;
- offering their customers the capacity to create, delete or deactivate vIBANs without the involvement of the PSP issuing the vIBAN and applying limited monitoring of the real use of these vIBANs (with direct access through an application program interface for example).

By contrast, the following indicators may indicate that a use case presents lower levels of ML/TF risk:

- a PSP servicing the master account has a direct business relationship with the end user of the vIBAN who is identified and verified;
- where the PSP servicing the master account and issuing the vIBANs is different from the PSP offering the vIBANs to the end users:
    - the PSP servicing the master account obtains due diligence on the end users of vIBANs;

- the PSP servicing the master account and the PSP offering the vIBANs to the end users are based in the same EU MS;

- the end users and the master account are based in the EU;
- a PSP offering vIBANs to the end users is an obliged entity under the AMLD and has effective AML/CFT systems and controls in place;
- a PSP has imposed limitations on the type of payments that can be processed via the vIBAN (e.g. to top up e-money account);
- a PSP servicing the master account restricts the provision of vIBANs to PSPs which are authorised agents only.