SECRETARIAT GENERAL

Anti-Money Laundering and Counter-Terrorist Financing Directorate

Cooperation and Analysis Department

A3 – Strategic Analysis

Overview and analysis of virtual IBAN services offered in France, from an AML-CFT perspective

March 2026

Table of content

STUDY PRESENTATION

In the course of its supervisory activities, the *Autorité de contrôle prudentiel et de résolution* (ACPR) has been confronted with the risks associated with virtual banking identifiers (also referred to as "virtual IBANs" or "vIBANs"), as well as with several high-risk use cases relating to this type of product.

Accordingly, in March 2023, the ACPR's AML/CFT Directorate conducted a study based on a questionnaire sent to 23 institutions (representing a sample of 14 credit institutions, 5 electronic money institutions and 4 payment institutions, both French and foreign, with a presence in France) concerning the use of vIBANs.

For the purposes of the review, vIBANs were defined as "the practice of combining several codes that have the formal appearance of IBAN (vIBAN) with a single payment account. Transfers to and from a vIBAN are in fact a transaction for this one master account". The questionnaire also targeted similar practices that would not exactly match this definition, especially those labeled as "vIBAN" or similar names such as "IBAN as a service". The questionnaire focused on vIBAN services involving France, i.e. when one or more of the following conditions is met:

- the master account has an IBAN with a French country code (FR),
- a vIBAN shows an FR code,
- a French entity supervised by the ACPR offers vIBANs to its customers (even vIBANs with foreign country codes, and even if the customers reside abroad),
- another entity of the same financial group offers vIBANs to French customers (even foreign vIBANs).

The preliminary findings of this review were shared with several peer foreign authorities, with a view to contributing to the work subsequently carried out by those authorities. These findings were also discussed with the ACPR's AML/CFT Consultative Commission.

In 2025, this report was further supplemented by case studies conducted by the French financial intelligence unit, Tracfin. These case studies illustrate use cases involving both French and foreign virtual IBANs, as well as certain risks associated with the misuse of this practice in financial schemes involving scams, fraud against public finances, money laundering, or the circumvention of sanctions.

SUMMARY

The survey shows that as of June 2023, 20 survey respondents were offering or planning to offer vIBAN services as described above [1], regardless of whether they use the terms of virtual IBANs. However for 2 of them vIBAN services purely rely on the use of multiple fully fledged accounts held by the establishment.

Virtual IBANs services generally consist in generating several IBANs used for routing payments to a unique payment account (sometimes called master account or main account), resulting in a single account appearing to have several IBANs.

The services described may aim to fulfill a specific use, or more commonly allow various uses decided by the customer. The vast majority of cases reviewed by ACPR involve legitimate uses, such as facilitating (i) reconciliation of payments (ii) analytical accounting (iii) payment factories within corporate groups.

However, as illustrated by the fact that some players offer similar services without relying on vIBANs, these objectives could be achieved by using a payment account per counterparty or per line of business, with automated rules (for instance, sweep accounts with any positive balance being automatically transferred to another account).

These services have been provided for around ten years in France.

The review also highlights the recent emergence of riskier use cases based on virtual IBANs such as (i) multiple re-issuance of vIBANs and (ii) provision of IBANs identified in a different country than the master account, which could be French or not. These vIBANs services appear to beused by criminal networks in order to bypass due diligence mechanisms, especially for cross-borders flows. Indeed, they obscure the actual destination of flows and undermine the ability of counterparties to adequately assess geographic risk. Depending on the circumstances, they may also complicate investigations conducted by the competent authorities, forcing them to multiply requests for international cooperation in order to obtain the necessary information. Thus, according to Tracfin, virtual IBANs whose country code does not correspond to the location where the master account is held present substantial vulnerabilities in terms of money laundering, scams, fraud against public finances, and the circumvention of sanctions.

At end-2022, the participants in the study reported:

- 1.7 million active vIBANs (0,7 million for client financial institutions, 0,6 million for clients that are non-financial companies; 0,4 million for individuals customers) ;
- 400 000 customers using vIBAN (including 18 financial institutions, 18 000 non-financial corporates, the rest being individuals) ;
- EUR 4 billion of transactions in one month (January 2023): 0,6 billion for financial institutions, 3,3 billion for non-financial corporates NFCs; 49 million for individuals.

The average number of vIBAN per customer varies widely: 40 000 per financial institution, 33 per non-financial companies and slightly more than one for individuals.

However, it is difficult to provide statistics per use cases, as financial institutions are not necessarily aware of their customers' purposes and several of those purposes can be combined (reconciliation and payment factories, for instance).

[1] Only 3 banks have no plans to offer this type of service, and one bank withdrew its offer in France in April 2023. Finally, two banking groups offer VIBAN services in other EU countries, but not currently in France.

This report describes in section I vIBAN uses with a low level of risk, followed in section II by high risk uses, and the ACPR's analysis of the applicable regulatory framework as well as the risk-mitigation measures addressing those risks (section III).

I – Low-risk services involving virtual IBANs

The vast majority of cases reviewed by ACPR involve legitimate low risk uses including to facilitate:

(i) the reconciliation of payments (assigning payments to counterparties, where each payer will be given a different IBAN),
(ii) analytical accounting (different IBANs used by different business lines);
(iii) the collection of payments on behalf of third parties (such as PSPs managing accounts for market places with multiple merchants, or "payment factories" collecting payment for multiple subsidiaries within corporate groups).

Financial institutions consider that the use , of vIBAN services can facilitate the monitoring of financial flows by providing the customer with an analytical view of his banking transactions, as each bank transfer can be categorized as soon as registered. VIBANs appears as a reliable way for automatically matching flows, as the account number is accurately carried over in payment messages, including across borders, whereas remittance information (such as invoice references) may be lost.

According to financial institutions the use of vIBANs can also enhance the traceability of internal transactions for both the customer and the financial institution servicing the payment account. Internal account monitoring procedures may therefore gain in speed and efficiency, by enabling the institution to retain a consolidated view of the customer's transactions on the master account.Respondents consider vIBAN as helping to reduce the risk of fraud, by avoiding the disclosure of the master account IBAN from third parties and restricting outgoing payments from vIBANs. The same result can, however, be achieved with two normal accounts.

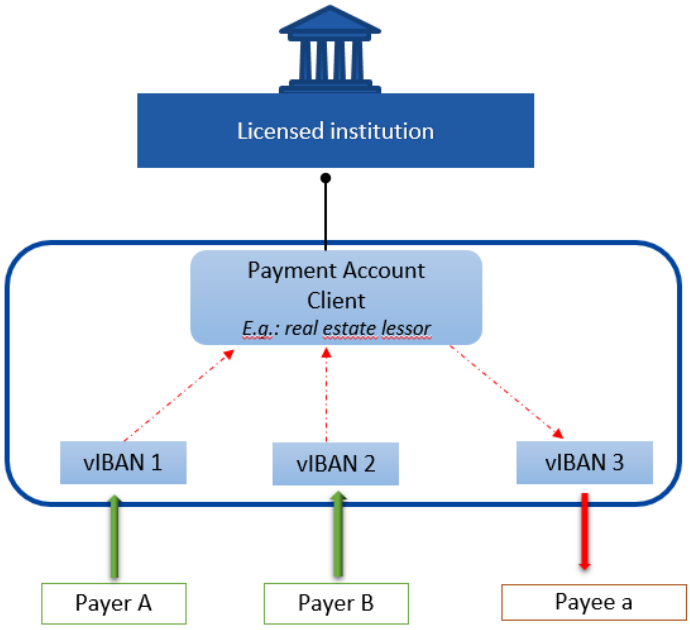
Case 1: Flows reconciliation

A different virtual IBAN is communicated by the financial institution's customer to each of its debtors (i.e. to each person from whom the customer expects a payment).

. Therefore, by seeing on which vIBAN third parties sent payments, the customer can automatically identify which payer sent the transfer. The reconciliation between financial flows and invoicing does not rely anymore on third parties manually filling of the "information field" of wire transfers (i.e. mention of an invoice reference, a name), or on analyzing the name of the payer. This facilitates for instance the identification of unpaid invoices. The revised Transparency of Funds Regulation may, however, reduce the needs for virtual IBANs, by mandating the use of company identifiers (for example, the "Legal Entity Identifier") to describe parties to the payment.

At the time of the study, three quarters of the respondents either provided or were considering supplying virtual IBANs services for reconciliation purposes. One institution offered a similar reconciliation service using payment accounts.

According to the results of the survey, the main subscribers of these services are entities receiving numerous-payments (such as real-estate lessors or marketplaces). The vIBANs are mainly used to distinguish between payers and segregate incoming credit transfers.



Case 1 – reconciliation of flows

Illustration No. 1: Use of virtual IBANs to facilitate the reconciliation of flows by an online casino or a crypto-asset service provider (CASP)

A foreign online casino may hold an account with a credit institution (CI) or a payment service provider (PSP), together with several virtual IBANs linked to that account. Each of these virtual IBANs may be assigned to one of its customers.
The online casino may therefore allow those customers to automatically fund their online gambling account by means of a credit transfer made to the virtual IBAN assigned to them. Upon receipt of the funds in its own account, the online casino credits the player's account with the transferred amount.

A crypto-asset service provider (CASP) holds an account with a credit institution or a payment service provider (CI/PSP), to which virtual IBANs are linked. These virtual IBANs are assigned to its own customers. As soon as the CASP receives a credit transfer on its account via one of these virtual IBANs, it credits the corresponding value in crypto-assets to the custodial wallet of the customer to whom the virtual IBAN has been assigned.

Case 2: Analytical accounting management[2]

A virtual IBAN is assigned to a subcategory of operations carried out by the customer acting on his own behalf. This type of service is offered in place of sub-accounts in order to provide an analytical view of transfers, which can be allocated to various categories defined by the customer, while simplifying the account structure.

It allows to reference a set of incoming and outgoing transfers using a specific IBAN. For instance, virtual IBANs can be used to segregate:

- a part of a business (business line, production line, …)

[2] 6 institutions offer this kind of services, and 3 intend to offer one.

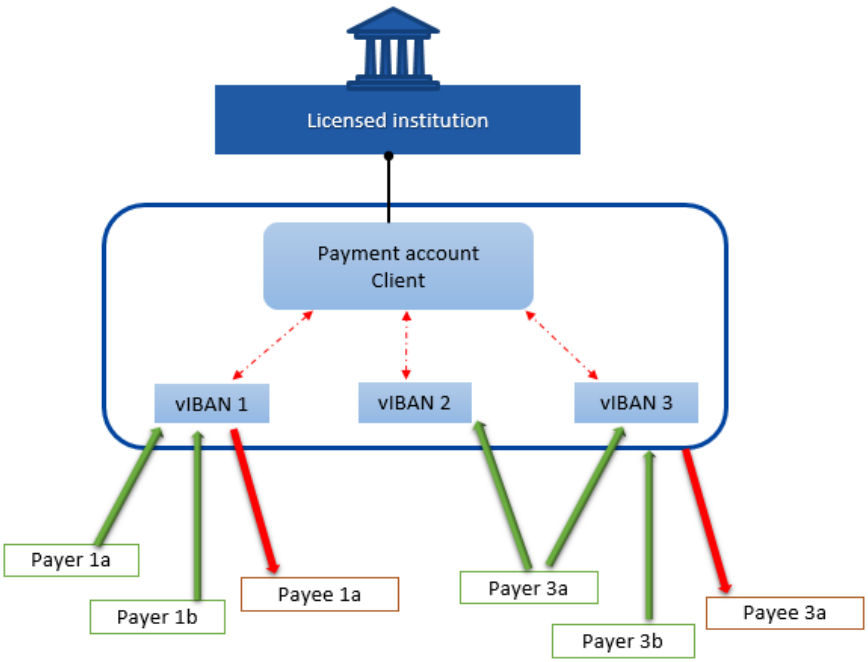
- an expense category (taxes, salaries, overheads)
- a type of customer (A customers, B customers);
- a tax regime (operations benefiting from a VAT exemption, or a specific VAT rate);
- flows by currency.

Most of the time, these use cases are for non-financial companies. In this kind of service, all the transfers are received or sent by the payment account owner on his own behalf.

Illustration No. 2: Use of virtual IBANs to facilitate the analytical management of flows by CARPAs

CARPAs (lawyers' escrow and settlement funds in France) use this type of service, for example, to create virtual accounts per lawyer and per case, thereby significantly facilitating account opening and the monitoring of transactions.

This service allows the customer to set up automatic management rules on a group of operations (as applying a VAT rate to a range of operations) or to classify transfers according to their currency.



Case 2 – analytical accounting

The use of virtual IBANs to facilitate payment reconciliation (Case 1) and analytical accounting (Case 2) by customers presents a similar level of risk.

➢ An overall low risk : increased complexity of transaction monitoring for third parties

These use cases present a low overall risk, limited to the fact that the use of vIBAN complicates the transaction monitoring for third parties (detection of many-to-one schemes more difficult, whereby mutliple payments that appear to be directed to different accounts are in fact ultimately intended for the same account).

Illustration No. 3 – Risks related to the circumvention of transaction-splitting detection mechanisms

An account may be associated with a large number of virtual IBANs. In order to prevent a significant transfer to an account from being detected by the originating bank's automated monitoring systems, such a transfer could be split into several transactions directed to multiple virtual IBANs linked to the beneficiary account (whereas multiple transactions directed to the same IBAN would be more readily detected). Such an operating model may, however, trigger other alert scenarios.

Some participants also indicated that they allow the use of virtual IBANs for outgoing payments. In such cases, the virtual IBAN appears in the payment message as the account from which the transaction is initiated. **It is therefore essential that the payment service provider complies with the regulatory requirements on the transparency of fund transfers, which require financial institutions initiating transfers to verify the accuracy of the information relating to the payer included in payment messages, in particular to ensure that the account number corresponds to the account from which the payment is actually made**.

Illustration No. 4 – Risks related to incomplete payment messages for third parties

Virtual IBANs may obscure the ultimate destination and actual use of funds. As in Illustration No. 1, PSP A provides virtual IBANs to CASP B, which assigns one to each of its customers. In certain cases, the ACPR observed that bank account identification statements associated such a virtual IBAN issued by PSP A with a customer C of CASP B, giving the appearance that the vIBAN corresponds to an account held by C.

This arrangement results in payment messages in which the beneficiary name is C, i.e. the end customer. As a result, the originating bank is able to identify the final recipient of the funds. However, this scheme has the drawback of obscuring the purpose of the transaction, as the beneficiary IBAN appears to belong to customer C. Indeed, if a transfer is made to an IBAN held in the name of CASP B, with an appropriate reference, the originating bank could assume that it relates to the purchase of crypto-assets and factor this into its transaction monitoring. Conversely, if the transfer is made to a virtual IBAN held in the name of an individual, for example its own customer, the bank may simply assume that the customer is multi-banked.

The issue of such hybrid chains, whereby a fiat payment ultimately results in the funding of a crypto-asset wallet from an economic standpoint, may be discussed within the FATF in the context of future guidance on the implementation of FATF Recommendation 16. Under the current legal framework, the payment message should indicate the name of the holder of the beneficiary account, namely CASP B.

In addition, when vIBANs are not in national account registries, authorities cannot access immediately useful information such as the verified payee name, account opening date and beneficial owners, added as a result of Anti-Money Laundering Directive 5.

➢ Possible mitigation actions

This risk can be mitigated as described here:

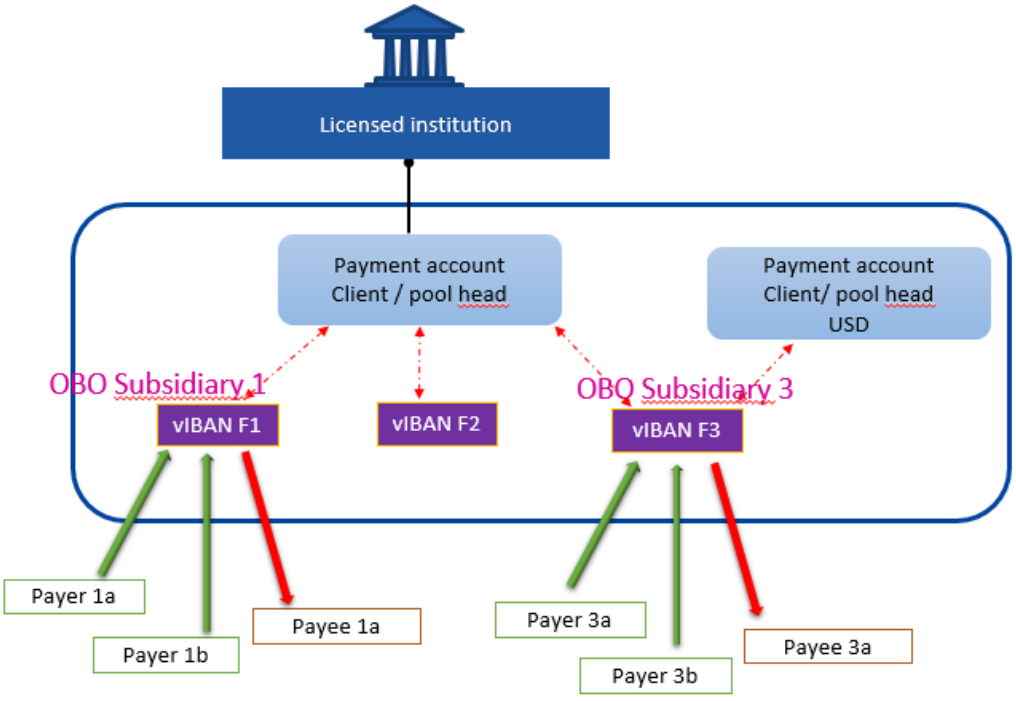
- Revised TFR mandating LEI/official identifier may facilitate identification of many-to-one schemes, but only for legal entities.
- Virtual IBANs services could be restricted to customers with a clearly justified business need, excluding customers exposed to a high risk of using such services for money laundering or terrorist financing purposes.
-

- Considering vIBAN as accounts that have to be in account registries, or or adding vIBANs in account registries as proxies of the "real" account number (This will be required by the 6th EU AML Directive, which will enter into application in 2027).
- the implementation of the revised FATF recommendation 16 should also mitigate risks as it requires beneficiary institutions to put in place mechanisms to verify that the beneficiary information contained in payment messages matches the information verified and held in their records.
- The use of the "ultimate beneficiary" field, in addition to the beneficiary field, in payment messages where supported (ISO 20022), could facilitate the identification of the end customer.

Case 3: Payment factories within corporate groups

One quarter of the respondents report they have been offering for several years vIBANs services that aim at facilitating payment factory management within corporate groups.

Each vIBAN is allocated to a separate subsidiary of a corporate group, and linked to the payment account opened by the cash pool head. The service enables the customer to facilitate the management of the flows it receives or sends on behalf of the companies it controls, while maintaining immediate visibility per subsidiary.



Case 3 – Payment factories

Illustration No. 5 – Use of virtual IBANs for payment centralisation purposes (payment factory)

Within a "payment factory" model, the customer of the credit institution / payment service provider is generally a corporate group seeking to centralise all transactions of its subsidiaries into a single

'master' account. Each subsidiary is assigned a virtual IBAN, the transactions of which are booked to the centralising account.

This model relies on so-called 'COBO' (collection on behalf of third parties) or 'POBO' (payment on behalf of third parties) functionalities. It may enable a reduction in account maintenance and account opening costs, the alternative being the opening of a separate 'real' account for each subsidiary.

The payment factories facilitation is presented by some establishments as a way to reduce account maintenance fees. These fees can be indeed reduced where the service provides for the provision of virtual accounts, as long as such accounts do not have a balance and do not incur the usual account fees. It should be noted that this reduction is even achieved at an institution which considers the accounts concerned as separate accounts, and seems to be more a pricing policy than a real cost saving.

These services may be combined with VIBAN services for accounting reconciliation or account management as mentioned above.

➢ A moderate risk provided mitigation measures are applied

This third use case presents a moderate risk, subject to the following caveats:

- The financial institution issuing vIBANs may not gather KYC about the subsidiary because it has no business relationship with the subsidiary. This seems acceptable only to the extent that the direct customer is entitled to receive funds on behalf of third parties and these accounts are not directly held or used by these third parties. The identification of the relevant group entities appears necessary in order to ascertain the ultimate beneficial owners of the transactions, pursuant to Article L. 561-2-2, 2° of the French Monetary and Financial Code."
- The funds operated could be misallocated to the subsidiary or the pool head.
- The use of vIBAN may blur country risk if cash pooling is cross-border.

Some respondents mentioned having implemented some measures to mitigate the risks:

- Some institutions restrict the vIBANs offers to corporate groups in order to avoid the risk that their customer could be seen as illegaly offering payment services, in case the necessary authorizations were not given.
- Such cash management services may be restricted to groups with ownership or solvency percentage requirements.
- Financial institutions commonly put procedures in place for checking capitalistic links and the reality of the corporate group, even collecting some form of KYC from the subsidiaries.

A key area of attention is whether the vIBANs are used by the cash pooling entity on behalf of subsidiaries, or by subsidiaries directly, as if they were their own accounts. If the latter, the use of vIBANs may cause a breach of KYC requirements and of the Transfer of Funds Regulation. The beneficial ownership requirements appear to be insufficient to mitigate this, as they focus on natural persons (rather than a web of subsidiaries) and do not carry the same verification requirements. .

* *

*

Analysis by the ACPR on these three use cases

In France, these initial three vIBAN use cases are permitted provided they are characterized as the provision of multiple accounts merged into a master account, the latter being assigned an IBAN and recording all transactions executed across the merged accounts. The ACPR requires such merged accounts to exhibit homogeneous characteristics and to be held by the same institution in the name of the same client. It should be noted that the ACPR's findings indicate that vIBANs are not systematically classified by financial institutions as accounts subject to mandatory reporting in the national register of bank accounts.

* *

*

II – High-risk services involving virtual IBANs

From an AML/CFT perspectives, two use cases of VIBANs services appear particularly risky:

- Case 4: re-issuance of vIBANs
- Case 5: the provision of vIBANs with a country code different from the country where the account is serviced.

Case 4: Cascading reassignment of virtual IBANs

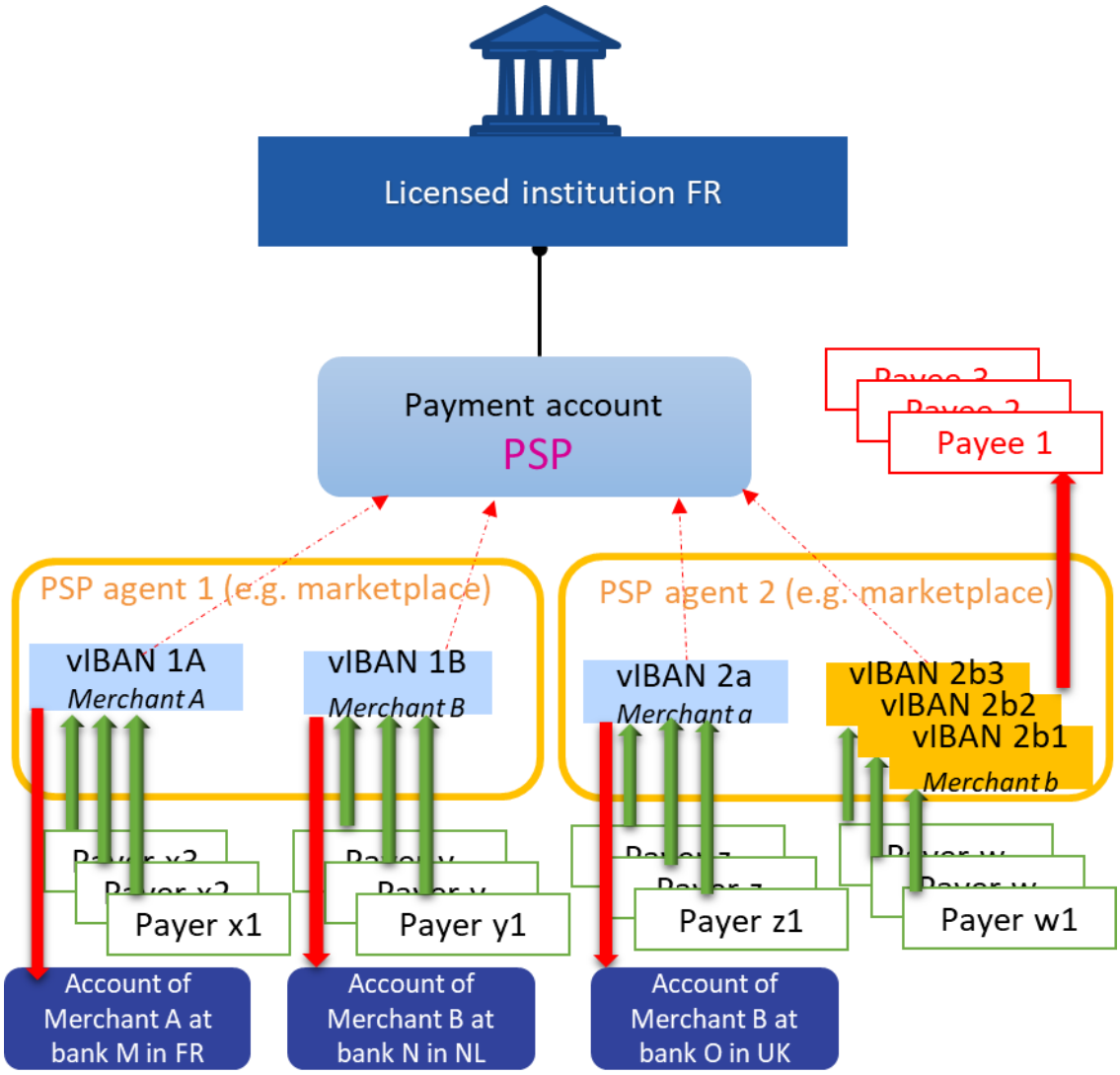
A few respondents offer vIBAN services to facilitate the collection of payments on behalf of their clients' underlying customers, within a contractual framework that does not involve the account-servicing institution. In contrast to the first use case described above, the terms of use for virtual IBANs allow the account holder (PSPs mainly) to re-issue the vIBANs to their own clients ("cascading" offer). The vIBANs distributed to the main account holder can be re-issued by successive PSPs, with no limit on the number of consecutive re-issuance. The number of intermediaries in the financial circuit can be high.

The ACPR has seldom encountered such cases in France, as French payment and electronic money institutions are issued their own interbank codes, and their IBANs feature this code to identify them.

One use case has been identified in particular, as provided by one respondent with a very large number of vIBANs users.

Re-issuance functionality could mainly be used by PSPs managing accounts for market places with multiple merchants (which may sometimes be PSP agents). Moreover, it allows crowdfunding platforms to collect payments for multiple project owners.

In the following scheme, the chain comprises three levels: a Credit Institution (CI) issues, on behalf of a client Payment Service Provider (PSP), a series of vIBANs linked to this PSP's account; this PSP then offers these vIBANs to its own clients, which are marketplaces in the following illustration



Case 4 – re-issuance in cascade

If a PSP assigns a vIBAN to one of its direct customer , for its own reconciliation needs, the risk level appears to be as low as in others cases of reconciliation services, as examined in the last cases. Nevertheless, in the above diagram, where a vIBAN is allocated not to the PSP's direct client (Marketplace 1) but to the latter's own customer (Merchant A) to facilitate the collection of payments from Payers X1, X2, and X3 intended for Merchant A, the risks are much higher.

Illustration No. 6 – Cascading Reassignment of Virtual IBANs

In the above example, the French authorized institution (the 'French Credit Institution') maintains no direct contractual relationship with Marketplaces 1 and 2, nor with Merchants A, B, a, and b, but performs due diligence solely on its direct client, the PSP. The PSP, which utilizes its accounts held with the French authorized institution to process payments received by its own clients, is responsible for conducting Customer Due Diligence (CDD) on these business relationships. However, situations vary from one marketplace to another:

> Certain marketplaces may act as the actual supplier of the goods or services sold and receive the payment into their own estate (Merchant A may merely be a supplier to the marketplace). In such cases, the PSP's client would be the marketplace itself.

> Others act strictly as intermediaries, connecting merchants with their customers. In this scenario, the merchants would also be considered clients of the PSP.

In practice, the PSP does not always correctly identify the true underlying purpose of the payments received and is unable to exercise effective monitoring over the flows (notably to ensure that such flows are consistent with its knowledge of the business relationship).

1) Risk of complexification of due diligence

- **Lack of information about the end-user of the vIBANs:** When the customer is a PSP and vIBANs are used for the operations of the customers of this PSP, the financial institution issuing vIBANs has no business relationship with vIBANs ultimate users. As a consequence, the issuing financial institution only gathers KYC elements on the PSP and none related to the end-customer to whom the vIBANs are assigned.

  The segmentation of due diligence between the financial institution servicing the master account and the PSP holding this master account may increase the level of risks. Risks are also higher when the ultimate customer obtains several vIBAN, in such a way that the activity of this ultimate customer is split across multiple bank identifiers.

Illustration No. 7 – Risks Arising from the Absence of a Direct Business Relationship with the End-User of Cascading Virtual IBANs

In this scenario, Institution A (identified by the bank code and country code of the virtual IBAN) may, depending on its internal policies and its agreements with its client, PSP B (which assigns the virtual IBAN to its own customer), only possess fragmented information regarding the end-customer.

Consequently, Institution A does not have access to the end-customer's account (it can only monitor transactions passing through the virtual IBAN and thus has only a partial view of the customer's operations with the PSP) and cannot contact the end-customer itself to request clarifications or supplementary documentation.

Thus, Institution A relies on PSP B for:

- Ongoing monitoring of transactions: Institution A lacks the necessary context to correctly identify suspicious transactions.
- Responding to inquiries from Financial Intelligence Units (FIUs) and other competent authorities regarding the vIBANs it provides to PSP B.

As a good practice, some institutions put procedures in place for collecting a lighter KYC from the end-customers. **A fragmentation effect on financial behavior**: The use of multiple vIBANs for a single end-user may complicate the ongoing monitoring of transactions. In such cases, it is necessary for the account-servicing institution toensure that the due diligence procedures applied by the account-holding PSP to its own clients enable effective oversight of the

transactional activity of each marketplace or merchant (specifically allowing for the reconciliation of all operations across the various vIBANs involved with the established customer profile).

Because of the similar structure of IBANs and vIBANs, institutions cannot detect the presence of a vIBAN, when receiving or sending funds from or to an external vIBAN. The transaction monitoring framework cannot therefore take into account the nature of vIBAN, as there are **no standardized references for vIBANs in the payment messages**.

Due diligence could be defeated by, for instance, allowing a customer to drop below manual transaction validation thresholds by **splitting transactions into multiple virtual IBANs**, whereas the cumulated amount of such transactions leading to a single IBAN would have triggered manual validation.

Most of the respondents to the survey do not implement specific due diligence measures on transactions recorded through vIBANs, considering transactions monitoring performed on the master account as adequate to cover all transactions. However, responses show that some institutions were not able to provide figures about active vIBANs.

2) Risk associated with the use of vIBANs as payment accounts

The use of virtual IBANs results in obfuscating the final recipient of the flows (when not the master account holder). For instance, a merchant's customer who initiates a transfer to the merchant may not know that the flows are received on an account which is not held by the merchant.

- **Unauthorized funds collection activity on behalf of third parties**: Virtual IBAN services are likely to facilitate the offense of unlawful exercise of the activity of providing payment services mentioned in Article L. 314-1 of the French Monetary and Financial Code, as they facilitate the reception of funds on behalf of third parties without being duly licensed or authorized as an agent.

  Some institutions rate the risk of fraud as low, because they restrict the use of vIBANs to incoming flows or restrict the vIBAN offer to legal entities registered as PSPs' agents, or on the contrary exclude PSPs altogether. Another bank specifically prohibits its PSP customers from distributing vIBANs as payment accounts. Some respondents monitor the abusive use of the vIBAN they issue: for instance, a suspicious transaction report was issued by one institution in January 2023 on this practice, where vIBANs were used by a customer to impersonate a PSP and make victims believe it could create accounts.

Illustration No. 8 – Facilitation of the Unauthorized Provision of Financial Services

Consider Entity A, holding an account that offers the capability to generate an infinite number of associated virtual IBANs. Since these vIBANs may possess an appearance and functionalities nearly identical to standard bank account details, Entity A can offer payment services to its clients—under a veneer of legitimacy—without the required regulatory authorization.

- **Use of vIBANs as actual payment account by third parties**: the main risk is that a vIBAN could be used by a third party as an actual payment account, without the third party being subject to AML/CTF due diligence. The vIBAN would then be the equivalent of an anonymous account.

The risks are particularly high when the services associated with the vIBAN resemble those of "normal" accounts, for instance when the end-user may, in addition to receiving payments:

- Issue documents that associate the vIBAN with names of third parties other than the verified account holder (in France: "relevé d'identité bancaire")
- have access to the equivalent of a vIBAN account statement, which may be facilitated by APIs allowing, for example, a marketplace to offer their merchant customers access to information about payments received by the market place on behalf of merchants (the confusion with a real account is particularly high if the virtual IBAN can have a balance);
- generate payments to third parties of its choice, again thanks to the practice of programmable interfaces, regardless of which account number appears as the sender (the confusion with a real account will be even greater if the virtual IBAN appears as the sender).

Illustration No. 9 – Risks Associated with the Use of Virtual IBANs for Outbound Transactions

Consider a virtual IBAN linked to an omnibus account held by PSP B with Credit Institution A. PSP B assigns the virtual IBAN to the account of one of its own clients, C. Client C uses this virtual IBAN to transfer funds to a third-party account, and its account with PSP B is debited accordingly. Since the debited customer account is that of C with B, the name of the original ordering party (C) should appear on the payment message, thereby complying with the 'Travel Rule': in this instance, the ML-TF risk is limited. Conversely, if PSP B's name appears instead, the risk is high, as the counterparty bank lacks visibility regarding the origin of the funds.

Many respondents offer their customers the capacity to create, delete or deactivate vIBANs with no intervention of the financial institution issuing the vIBAN, and limited monitoring of the actual use of these vIBANs.

Ways to mitigate these risks include:

- considering vIBANs as actual payment accounts, and subjecting their holders to AML-CFT due diligence obligations by their respective PSPs; **the ACPR considers that many of the so called "vIBANs" are actually full payment accounts**;
- Making sure that payments are intended for the master account holder itself (marketplace or real estate agent), or that such master account holder is duly authorized to collect payments on behalf of third parties ;
- Restricting outgoing payments solely to the vIBAN user's other accounts (to the exclusion of third-party payments): for instance, in cases where vIBANs are allocated to each merchant on a marketplace, outbound payments would be restricted to each merchant's own account held with another payment service provider.

The ACPR considers the cascading reassignment of virtual IBANs to be a particularly high-risk practice.

Case 5: Provision of vIBANs whose country code differ from the country where the funds are held

Some virtual IBANs services can be used to carry out transactions which are routed to a main account held in another country. Thus, vIBANs have a different country code from the ultimate payment account. Some "IBAN services" consist in allowing customers to have accounts with different country codes although the PSP considers that the accounts are all in the same country. The vIBANs can be

issued either by a partnership with a local partner institution (case 5a), or by a local branch of the same establishment (case 5b).

Respondents consider these services reduce the account management fees, with a lower cost of virtual IBANs than sub-accounts. VIBANs also allow to offer local payment options, in local currency, in different countries, reducing the cost of currency change. In this way, transactions can be carried out more quickly and at lower exchange rates in the countries concerned, by being processed by local payment networks. Lastly, local IBANs can be more easily accepted by counterparties and help avoid discrimination based on the country in which the IBAN is issued.

Unlike other vIBAN services, the number of vIBANs provided is usually one per customer and per country code. The creation and use of vIBANs usually rely on an automated process with no intervention of the financial institution. **Illustration No. 10 – Use of 'Multi-Country' Virtual IBANs by Merchants Operating Across Multiple Jurisdictions**

A merchant based in Third Country B wishes to sell its products efficiently within the European Union but seeks to avoid the costs and complexities associated with a banking relationship with a European bank. The merchant opts for a PSP in Country B that offers virtual IBANs from European Country A (country code 'AA'). This PSP is not established in Country A but has opened an omnibus account with a bank in Country A, linked to 'AA' virtual IBANs. The PSP assigns one of these vIBANs to the merchant in Country B. Funds transferred by the merchant's customers to this vIBAN are deposited into the PSP's omnibus account in Country A. The PSP subsequently credits its client's account in Country B, or may even allow the 'AA' vIBAN to maintain a balance in the 'AA' currency**.**

The survey points out two vIBAN or "IBAN services" models disconnecting the country code of the vIBAN from where the funds are held. The risks for both models will be examined below. While the use cases are limited to very few institutions, those receive some 20% of the value of fraudulent wire transfers in France (as measured by recalls).

5.a - Provision of foreign vIBAN linked to a French account

The first model consisted , for the French branch of an EU financial institution, in providing its customers with a French account together with additional IBANs that have foreign country codes, for instance for currencies other than the euro. Payment operations were initiated directly by the French customer from this virtual IBAN to external beneficiaries, with the references of this vIBAN mentioned in wire transfers and account statements.

Each vIBAN referred to the BIC of two foreign partner institutions licensed in another EU Member State. These partners provided the French establishment with a payment account (called omnibus account or "pool account" below). Funds sent to the vIBANs are held on those omnibus accounts. Accounts statement by the French branch's accounts bore the appearance of fully-fledged accounts, featuring distinct account numbers and separate balances.

Illustration No. 11 – Provision of Multi-Currency Wallets in the Form of Virtual IBANs

Providers of multi-country virtual IBANs frequently combine this offering with multi-currency management capabilities. This results in as many virtual IBANs (or other account identifiers for non-IBAN jurisdictions) as there are currencies: for instance, a PL IBAN for payments and collections in zlotys, a GB IBAN for pound sterling, and a BE IBAN for euros. These multi-currency products typically offer foreign exchange (FX) services between the supported currencies. Such products allow for foreign exchange risk management; for example, a corporation or an individual expecting to make future payments in a specific currency can convert funds in advance and hold them in that currency.

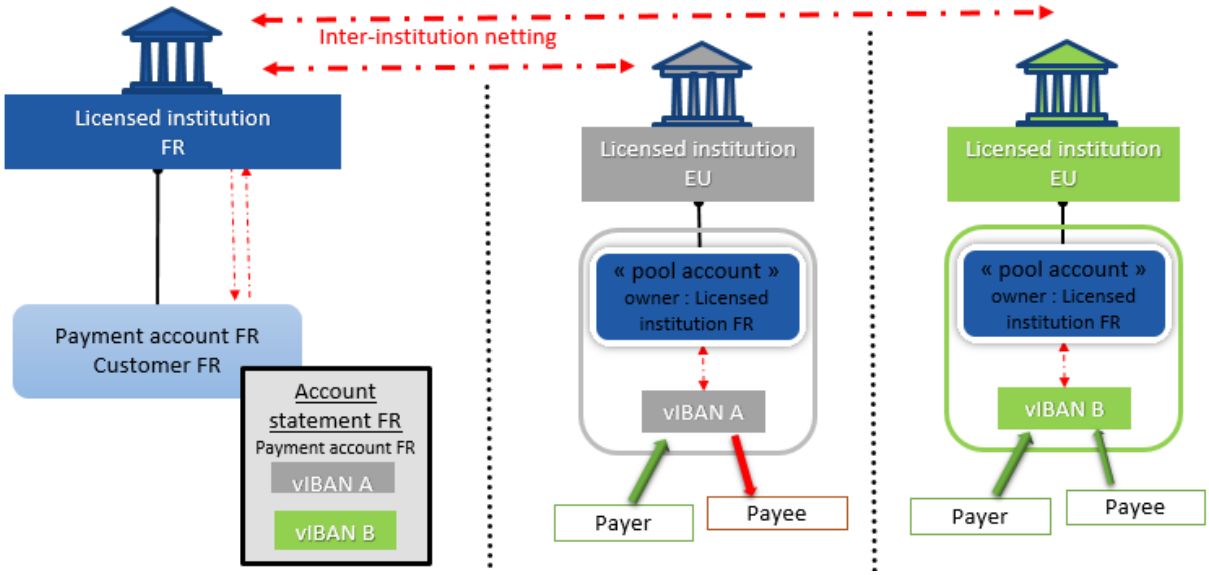
They also serve to avoid FX fees when payments received in a foreign currency are offset by outgoing payments in that same currency.

However, they may also lend the appearance of a domestic payment to what is actually an international transaction, thereby circumventing regulations implementing FATF Recommendation 16 on the transparency of wire transfers. Consequently, in the revision of this Recommendation published in June 2025, the FATF included a new paragraph 7 in the Interpretive Note, which specifically prohibits the use of account numbers to obscure the identification of the country where the account-servicing financial institution is resident.

The ACPR considers that these so called vIBANs are in fact genuine payment accounts offered in France by the other EU institutions through the French entity. In addition to the due diligence obligations incumbent upon the aforementioned European institutions, any French institution shall also be required to exercise vigilance over the products it helps distribute and to take into account all available information when conducting due diligence on its clients.

Respondent consider that the use of vIBANs facilitate the reconciliation of collected flows in local currency on behalf of its customers, avoiding to rely on wire transfers references, PSPs assistance, or pooled account solutions.

Another similar offer was also withdrawn from the market at a point in time closely coinciding with the period in which the inquiry was conducted.



Case 5a – Foreign virtual IBAN linked to a French payment account

* *
*

The ACPR categorizes case 5a as fully-fledged payment accounts maintained by the foreign partner institutions.

These foreign vIBANs are provided to the French institution and utilized to offer accounts in other currencies to French clients; however, they are in fact fully-fledged payment accounts provided by the foreign institution, which should apply all AML-CFT obligations to the account holder.

5.b - Provision of a French vIBAN linked to a foreign account

Several institutions have opened branches in France in order to issue French IBANs, which led to confusions:

- in some cases, the same account had several IBANs or vIBANs with different country codes, which were used to route payments to the main account. **The ACPR made clear that this was not possible, as the same account cannot be in several countries.**
- in other instances, the institution considered that the account with a French IBAN was held in another country. **The ACPR made also clear that under the ISO standard governing the IBAN, the country code should reflect the country where the account is, including the country of the branch if the account is maintained in a branch**.

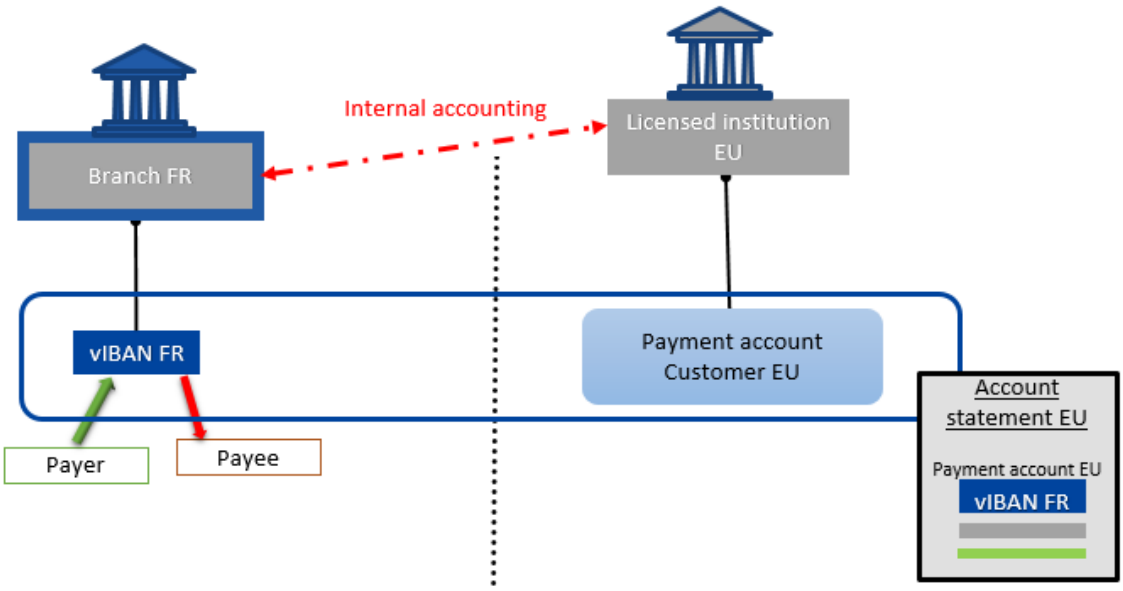
This does not prevent the use of sweep accounts: these notably include standalone payment accounts where a transfer is automatically executed to an overseas account each time the French account is credited. Such practice is high risk and requires enhanced monitoring, as changing jurisdictions is a way to obfuscate the flow of funds. These automated cross-border transfers are also used by fraudsters in various types of wire transfer fraud[3] to avoid alerting the victim and complicate the efforts of law enforcement authorities.

Illustration No. 12 – Risks Associated with Virtual IBANs Issued by a Branch for Accounts Maintained by a Foreign Parent Company

When a virtual IBAN is generated by one entity of a payment service provider group while the master account is held by another entity of the same group abroad, ML-TF risks depend on the quality of intra-group information sharing. For instance, if the branch has consolidated access to the transaction flows on the account held by the other group entity, exercises oversight over these flows, and reports to the Financial Intelligence Unit (FIU) of its country of establishment, the risks are mitigated.

Therefore, the French branch should have access to information on the other accounts or vIBANs held by the same customer in other branches or entities of the same group, including the head office. Indeed,an isolated analysis of transactions processed solely through the French vIBAN does not provide a comprehensive understanding of the overall business relationship : this prevents for instance detecting that social benefits paid in France are immediately withdrawn in cash abroad, or that incoming wire transfers received on the French IBAN of a company are immediately wired onwards, without any sign of real economic activity such as paying rent, taxes, salaries and social contributions.

[3] For instance, investment scams where the fraudster will impersonate a French financial institution ; various forms of phishing or email fraud where fraudsters divert payments intended for third parties such as suppliers, notaries.



Case 5b– Virtual IBAN FR linked to a foreign payment account

As mentioned above, some respondents justify such products by the circumvention of IBAN discrimination. Such discrimination is illegal and subject to sanctions by the competent French authorities . Accepting to disguise in a vIBAN the true location of funds goes against several pieces of European legislation, and affects important objectives, including the fight against money laundering, terrorism financing and tax evasion.

The issuance of French vIBAN services linked to a foreign master account is accepted by the ACPR under the following conditions:

- **The vIBANs are characterized as payment accounts, the management of which is ensured by the French branch, which has real-time access to all transactions carried out by the client;**
- **Client assets are recorded in the French branch's accounts and can be seized in France by law enforcement authorities;**
- **The branch applies French AML-CFT laws and regulations as well as the asset-freezing regime, and files suspicious activity reports with the French FIU.**

The application of these principles is fully compatible with:

- **The outsourcing of tasks such as IT management, transaction monitoring, and accounting to another country, resulting in the branch employing only a limited number of permanent staff on French territory, provided that the French branch possesses sufficient resources and expertise, and that the ACPR has access to all information and personnel to carry out its supervisory activities.**
- **Redirection accounts, where funds are automatically transferred to the foreign account upon receipt by the French account, and automatically transferred from the foreign account to the French account when a payment must be executed: these automated rules can achieve the same effect as virtual IBANs while ensuring compliance with laws and regulations. These cross-border redirection accounts are very-high-risk products requiring enhanced due diligence and a consolidated view of all accounts or vIBANs. The French branch should have consolidated information to fulfill its AML-CFT obligations, notably to conduct**

enhanced examinations and to file suspicious activity reports with the French FIU, under the supervision of the ACPR.

These situations are sometimes presented by the relevant institutions as 'payable-through accounts' which allow client C of financial institution A to execute transactions directly on the account of financial institution A opened with correspondent institution B. In this case, regulations impose enhanced due diligence as set out in Article R. 561-21 5° of the CMF. However, this enhanced due diligence does not replace the obligation to conduct full customer due diligence (KYC) on client C in the case of a vIBAN assigned to each client that redirects to a foreign account held by that client.

5.c – Illustrations of risks associated with French vIBANs linked to a foreign account

The use of a vIBAN to obscure the actual location of funds contravenes several European legislative acts with significant implications, particularly regarding the fight against money laundering, terrorist financing, and tax evasion.

1) Risk affecting the assessment of geographic risks

The use of vIBANs with a different country code from the main account, or IBANs with the wrong country code, results in inaccurate information about the country in which the account is located and, in consequence, about the actual source or destination of funds. Third parties cannot identify the relevant national legislation and supervisory authority, which distorts the assessment of geographic risks and prevents the implementation of additional due diligence measures for transactions involving higher risk countries. For instance, wire transfer fraud is significantly higher for payments to certain EU members. Criminal networks may use a local IBAN in order to facilitatescams , because victims are less careful when they believe they are sending funds locally.

Illustration No. 13 – Risks Associated with the Neutralization of Geographical Due Diligence Criteria

The proliferation of cross-border transfers without apparent economic justification is a useful analysis and alerting criterion for detecting shell companies and money laundering operations, particularly for the institution holding the account of the entity issuing the transfers. The use of local virtual IBANs can partially neutralize this analysis criterion: cross-border transfers appear to be domestic transfers due to the country code of the recipient IBANs. While the institution can still detect suspicious account activity based on the lack of economic justification for the transactions, it is deprived of the geographical criterion, which is both useful and easily automated.

The neutralization of the geographical criterion can also affect the work of Financial Intelligence Units (FIUs), particularly when the prioritizing and assigning cases.

2) Risks regarding the implementation of targeted financial sanctions

Misleading country information in an IBAN also results in:

- **Uncertainty on applicable targeted financial sanctions:** The financial institutions need to identify the country where an account is legally serviced in order to apply relevant targeted financial sanctions screening. Indeed, sanctions lists are not harmonised at EU level, and national sanction lists may exist according to Resolution 1373 (2001) of the United Nations Security Council and the FATF's Recommendation 6. Uncertainty may result in litigation and is therefore a source of legal risks for the financial institution managing the account.

- **Uncertainty as to whether a transaction is cross border or not and about screening obligations of third parties**: In France, financial institutions rely on the country code to determine whether the transaction is within the French territory and exempted from sanction screening[4].

Illustration No. 14 – Risk of Sanctions Evasion through the Use of Virtual IBANs

The geographical analysis criterion is critical for detecting cases of sanctions evasion:

- The destination country of the funds may be under sanctions, or known to host natural or legal persons subject to sanctions.
- The destination country may be known for not enforcing the relevant sanctions (a substantial issue, particularly for sanctions decided at the national level).
- The use of FR virtual IBANs linked to a master account held in another country could create the illusion of a transfer executed entirely within national territory, thereby circumventing the screening obligations applicable in France.

This risk has seen little materialization at this stage; however, one case was brought to Tracfin's attention: Institution A in European Country A provided PSP B with a virtual IBAN from Country A. PSP B had assigned this IBAN to a company offering services that could fall under European sanctions. The virtual IBAN in question was blocked.

3) Obfuscation of the country where the account is held

- **Wrong IBAN country codes jeopardize the correct implementation of several pieces of EU law that rely on the bank identifier's country code.**

Several EU regulations beyond AML/CFT rely on the link between the IBAN country code and the country where the accounts are legally serviced, with the clear understanding that the IBAN country code reflects where the funds actually are.

For instance, EU rules on cross-border **debt recovery in civil and commercial matters**[5] uses the IBAN country code to determine in which Member State the account is maintained. The same goes for Article 2 of Regulation 2015/848 on **insolvency proceedings**[6]**.**

[4] France admits that national transfers - between accounts with a French IBAN - are not subject to sanction screening against French sanctions at transaction level, as all parties to the payment are already screened. This would be jeopardized if the country code becomes meaningless, when transactions between two accounts with a French IBAN are in fact international transfers, with no guarantee that PSPs involved in the transfer are screening their customers against the lists applicable in France.

[5] Regulation 655/2014 (Art. 4) establishing a European Account Preservation Order

[6] "(9) 'the Member State in which assets are situated' means, in the case of : (…) (iii) cash held in accounts with a credit institution, the Member State indicated in the account's IBAN, or, for cash held in accounts with a credit institution which does not have an IBAN, the Member State in which the credit institution holding the account has its central administration or, where the account is held with a branch, agency or other establishment, the Member State in which the branch, agency or other establishment is located."

Another EU mechanism aiming at **combatting VAT fraud**[7] relies on the IBAN of the payment accounts involved in the transfers, or the BIC of the PSP acting on behalf of the payer or the payee, to gather information about cross-border transfers.

The automated exchange of information framework between national tax authorities may be undermined by the use of bank identifiers featuring a country code that differs from the country where the master account is held: intermediate financial entities must identify the country in which a foreign payment account is maintained in order to comply with their automated exchange of information obligations for tax purposes, as 'Reporting Financial Institutions' within the meaning of the OECD Common Reporting Standard (CRS), implemented in the EU through the Directives on Administrative Cooperation.

- **Wrong IBAN country codes misdirect FIUs and law enforcement:**

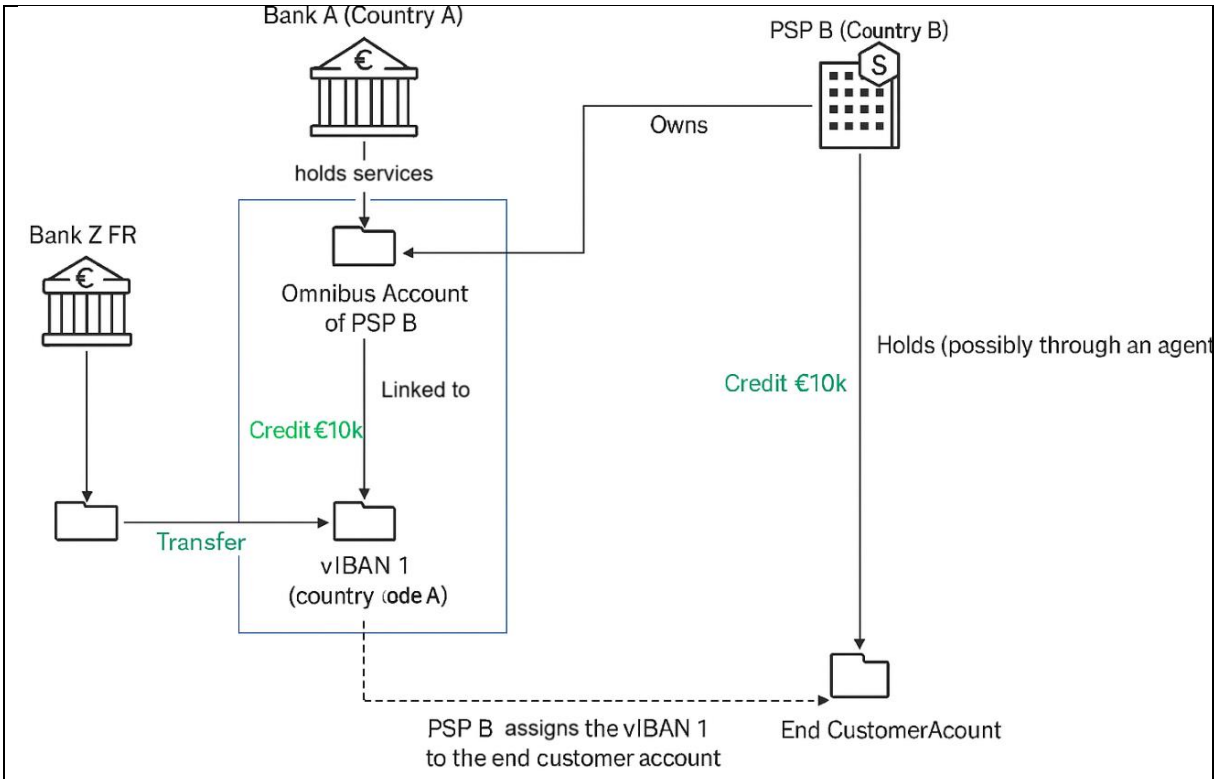
Legal procedures will be misdirected if third parties are led to believe that an account exists in a given establishment and a given country, when the actual account is elsewhere.

- The risk lies in the misdirection of requests from competent authorities: public authorities must be able to quickly and reliably identify which institution maintains the account and in which country. They are abused by the use of vIBANs with the wrong country codes, leading to procedures being misdirected, and losing precious time which can compromise their actions . Responsiveness is an even more pressing issue with the development of instant payments. For instance, in cases of fraud, swift action is essential to recover funds.

Illustration No. 15 – Risk of Extended Investigation Timelines Due to the Use of Virtual IBANs

The disconnect between, on the one hand, the institution identified by the IBAN's bank code and country code and, on the other hand, the institution with full visibility over the client and the account, can lead to significant investigation delays.

[7] The Directive (EU) 2020/284 of 18 February 2020 amending Directive 2006/112K (CESOP -Central Electronic System of Payment Information- established to combat VAT fraud) requires PSPs to retain and provide information in relation to cross-border payments, defined as payments between a payer located in a Member State and a payee located in a Member State, a third territory or a third country.



In the event that a bank in Country A generates virtual IBANs for the omnibus account of its client, a PSP in Country B, and the latter reassigns these virtual IBANs to its own clients (with accounts maintained in Country B), the French FIU may seek to obtain information regarding the user (the end-client) of one of these virtual IBANs, specifically the client's account statement, in order to track the flow of funds. Based on the bank code and country code, the French FIU queries the FIU of Country A. The FIU of Country A then forwards the request to the bank in Country A. In practice, the latter generally does not possess the requested information: only the PSP in Country B, which maintains the actual account of the end-client, can provide it.

The bank in Country A can:

- In the best-case scenario, obtain the information requested by the French FIU by soliciting its client, the PSP in Country B, within the framework of their contractual relationship.
- In the worst-case scenario, inform the FIU of Country A that it does not have the requested information, and that the French FIU should instead query the FIU of Country B, which would then be in a position to query the PSP in Country B directly.

In both cases, the investigation suffers an additional delay (potentially much more significant in the second scenario).

In this example, the virtual IBAN could functionally be compared to a taxi account in Country A, with two key differences:

- Instead of having to establish a relationship with two institutions (the PSP in Country B and the bank in Country A), the end-client only establishes a relationship with the PSP in Country B: they are thus subject to fewer due diligence measures.
- While the typical operation of a taxi account could be detected by the bank in Country A, a virtual IBAN does not allow for such an analysis (since the very purpose of a virtual IBAN is to transfer all funds to the actual account to which it is linked).

- **Misdirecting account seizures/restraints, with an impact on delays:** French police officers can seize a French account immediately, subject to subsequent confirmation by a judge, while seizing an account in another EU country requires a judge and takes at least a few days.

Illustration No. 16 – Risk of Public Finance Fraud

In the context of fraud targeting public aid schemes restricted to national territory, fraudsters may use a virtual IBAN to establish the credibility of their eligibility. As with the aforementioned scams, the master account is maintained in a country where the funds will be very difficult to recover. This was notably observed during the COVID crisis.

4) The obfuscation of the origin and destination of flows facilitates money laundering

When multi-country IBANs are attached to an account, virtual IBANs can be misused to disguise the true source, location or movement of property, which is one of the components of the money laundering offense, as defined in Article 3 of Directive 2018/1673 (L_2018284EN.01002201.xml (europa.eu)).

Illustration No. 17 – Fraud Risk

In a fraud scenario, a scammer established in a third country (Country A) may use a virtual IBAN with a European country code—where the destination account is held by a PSP in Country A—to defraud European victims. Both the client and their bank are reassured by the European IBAN (which can also lend credibility to the scammer's fabricated story), but the funds are actually paid into an account maintained by the third-country PSP. This applies, for example, to Business Email Compromise (BEC/FOVI) scams or investment fraud. Cases of this nature have been handled by Tracfin.

As a matter of fact, **institutions offering accounts with multiple country codes are more exposed to money laundering:** The few institutions offering various forms of multi-country IBANs represented some 20% of the value of wire transfer recalls for fraud in France in 2022, although those players represented less than 0,5% of payments received in France.

Illustration No. 18 – Complex Money Laundering Scheme Involving Virtual IBANs

Tracfin investigated a money laundering circuit linked to fraud involving several French virtual IBAN providers and multiple 'multi-currency wallet' providers specializing in international payments.

1. Funds were first transferred to accounts held in France with several online banks, as well as to French virtual IBANs. The accounts associated with these virtual IBANs were maintained in various European countries.

2. Subsequently, the funds were notably transferred to other European multi-currency wallets and then transferred again toward accounts held in third countries with poor cooperation regarding AML-CFT.

The combination of virtual IBANs enables complex and opaque capital transfers: financial movements that appear to be domestic may not be so, and a transfer that seems destined for a European country may in fact be exiting toward a jurisdiction with lower AML-CFT standards. These mechanisms obscure the origin and destination of funds, complicating both the monitoring obligations of financial institutions and the investigative work of administrative authorities.

5) Misleading consumers about deposit insurance mechanism

The customer might think that it has several accounts at several institutions (different country codes and institution codes), each eligible for the deposit insurance cap, whereas the PSP considers that the customer only has one account.

Furthermore, although European laws have been harmonized, the location of accounts servicing still has consequences because of remaining differences in national implementation, and because it determines which scheme should be the contact point of the customer.

Table summarizing the risks associated with the use of virtual IBANs

		Risks	Mitigating measures used by some establishments
Low-risk cases	**CASE 1** Payment Reconciliation	▪ More complex due diligence by third parties on the financial transactions due to the fragmentation of the customer's financial activity between multiple account identifiers (detecting "many to one" schemes becomes more difficult). ▪ Non-compliance with regulations on the transparency of transfers of funds, in the event of outgoing flows sent from a virtual IBAN.	Limiti the offering of vIBAN to companies presenting a clear use case, while excluding cases where the vIBAN is likely to be used for money laundering purposes. . The use of Legal Entity Identifier (LEI) in payment messages might also be a mitigating factor in the future. Implementation of obligations to report virtual IBANs to the national bank account register. Inclusion of both the virtual IBAN and the master account IBAN in payment messages (provided this can be done in a standardized manner that is understandable to third parties).
	CASE 2 Analytical accounting	▪	
	CASE 3 Payment factory	▪ Insufficient KYC collection by the vIBAN issuing institution. ▪ Possible accounting offenses or tax offenses in case of misallocation of the funds in the subsidiary's accounting ▪ Illegal exercise of account-keeping activities by the holder of the vIBAN master account. ▪ Concealment of geographical risk if the payment factory includes entities located in several countries.	▪ Use of vIBANs restricted to corporate groups for which capitalistic links and the reality of the corporate group have been verified. ▪ Verify that the head of the payment factory is authorized to receive funds on behalf of its subsidiaries. ▪ Collecting subsidiaries' KYC ▪ Exercise due diligence regarding the use of virtual IBANs and the allocation of funds to the payment factory.

High-risk cases	**CASE 4** Re-issuance of virtual IBANs	▪ Virtual IBANs users have no direct business relationship with the institution issuing the vIBANs ▪ Lack of KYC collection by the vIBAN issuing institution ▪ Obfuscation of the identity of the real user of the account ▪ Increased complexity of transaction monitoring for the account-servicing institution as well as for third-party institutions. ▪ Can allow money-collecting activity on behalf of third parties without any authorization ▪ ▪ Use of virtual IBANs as actual payment accounts by third parties ▪ Appearance to third parties of a payment account opened in the user's name, based on the information provided in payment messages and statements.	▪ Classification as a payment account, reported to the national bank account register as a standalone account (this reporting requirement is integrated into the EU AML6 package). Prohibition to distribute vIBANs as payment accounts and use of vIBANs restricted to flows collection with KYC on effective users of the vIBANs ▪ Restric vIBANs to PSP or authorized agents only ▪ Limit and monitor the number of virtual IBANs issued. ▪ Restrict the counterparties authorized to receive outgoing flows ▪ When the client is a PSP, collect general information on the AML-CFT due diligence measures applied by the client PSP to its own customer base, and implement collaboration procedures for performing such diligence ▪ Ensure that payments are intended for the master account holder itself (e.g., a marketplace or real estate agent), or that this third party is authorized to collect payments on behalf of third parties

	CASE 5 a and b Different country code IBAN/payment account	▪ Obscures geographic risks for third parties; ▪ Non-compliance with financial sanctions by the issuing financial institution and third party institutions; ▪ Misdirection of FIUs and law enforcement: requests sent to the wrong country. ▪ Jeopardizes the correct implementation of several pieces of EU law, including debt recovery, insolvency proceedings, and the CESOP scheme to combat VAT fraud ▪ Risk of confusing consumers about the implementation of deposit insurance schemes (the customer might think that it has several accounts at several institutions, each eligible for the cap, whereas in reality it only has one account)	▪ Use of real accounts as sweep accounts, when there is an established economic rationale and with adequate monitoring commensurate the high risk level; ▪ In the absence of alignment between the country code and the country where the account is held, virtual IBANs should be analyzed as payment accounts. They are then considered redirection accounts, classified as high-risk. Like any account designated by a French IBAN, a virtual IBAN issued under the 'FR' country code must be managed under the responsibility of the French entity; client assets are recorded in the French entity's accounts and are subject to seizure therein. The entity applies French laws and regulations regarding AML/CFT and asset freezing regimes, and submits suspicious activity reports (SARs) to the French FIU. Consolidated view of related accounts across entities

III – ACPR analysis of regulations and risk mitigation practices related to virtual IBANs

1) Recent Regulatory and Legislative Developments

The benefits and risks associated with the use of virtual IBANs have been studied by numerous authorities since 2023:

- In a report published in 2023, Europol[8] warned of the risk that criminal networks might exploit the complexity resulting from virtual IBAN usage to obscure the origin of illicit funds;
- In November 2023, the FATF[9] published a report highlighting the risk of misuse of virtual IBAN services, insofar as fund traceability is reduced by the lack of a fixed physical location and flow redirection features;
- In May 2024, the European Banking Authority (EBA) published a report[10] dedicated to virtual IBANs, which emphasizes the transparency and regulatory issues raised by the obscuring of the actual location of funds and the identity of end-users when virtual IBANs are utilized. The ACPR contributed to this report, notably through the present study;
- Consistent with this report, the Bank of Italy[11] published recommendations regarding virtual IBANs, and the German supervisor (BaFin)[12] has been conducting a thematic review since early 2025 to evaluate the usage of virtual IBANs.

In parallel with these efforts, some clarifications have been introduced at EU level:

Regulation 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[13], which will apply from 10 July 2027, defines "virtual IBAN" as "an identifier causing payments to be redirected to a payment account identified by an IBAN different from that identifier" (Article 2).

Article 22 of that regulation states that "*Credit institutions and financial institutions shall obtain information to identify and verify the identity of the natural or legal persons using any virtual IBAN they issue, and the associated bank or payment account.*

The credit institution or financial institution servicing the bank or payment account to which a virtual IBAN issued by another credit institution or financial institution redirects payments, shall ensure that it can obtain from the institution issuing the virtual IBAN the information identifying and verifying the identity of the natural person using that virtual IBAN without delay and in any case within 5 working days of it requesting that information."

[8] Europol (2023), European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime, Publications Office of the European Union, Luxembourg.
[9] Financial Action Task Force (FATF), Illicit Financial Flows from Cyber-Enabled Fraud, November 2023.
[10] European Banking Authority (EBA) (2024), Report on Virtual IBANs, EBA/Rep/2024/08, May 2024. EBA Report on virtual IBANs.
[11] https://uif.bancaditalia.it/pubblicazioni/comunicati/documenti/Comunicazione-BdI-UIF-vIBAN.pdf
[12] Vedrenne, Gabriel. "German Regulator Targets Virtual IBANs." MoneyLaundering.com, 28 January 2025.
[13] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401624

In addition, Article 16 of Directive 2024/1640, which has to be brought in to national law by 10 July 2027, requires that virtual IBANs be included in the bank account registers, including "*the virtual IBAN number, the unique account identifier of the account to which payments addressed to the virtual IBAN are automatically redirected, and the dates of account opening and closing*". The text further clarifies that "*In the case of a virtual IBAN, the customer account holder as referred to in point (a) of the first subparagraph shall be the holder of the account to which payments addressed to the virtual IBAN are automatically redirected*."

ACPR is presenting here its approach to vIBANs, meant to apply existing EU legislation, and that the ACPR views as compatible with the new pieces of legislation described above, while taking into account requirements, under Regulation 2023/1113 (Transfer of fund regulation) and the SEPA regulation

Furthermore, several possible additional avenues for the evolution of law or international standards regarding vIBANs have been identified:

■ Useful information in bank account registers

The obligation to reference virtual IBANs in bank account registers, established by the 6th AMLD (Anti-Money Laundering Directive), will provide greater transparency.

In cases where the holder of the account directly associated with the virtual IBAN is another financial institution (credit, payment, or electronic money institution, or a similar status abroad), the following data could be made available:

- Data on the account holder, i.e., the institution maintaining the end-client's account. This data includes the country where it is established.
- KYC data on the end-client (user).

The 6th Directive also allows Member States to require that other information deemed essential to FIUs be accessible and searchable (Article 16§6), even if such information may not benefit from the interconnection between European registers (Article 16§7). In this regard, it could be useful to include in these registers:

- The identity of the vIBAN user, in addition to that of the account holder; this information must be collectable pursuant to Article 23§3 of Regulation (EU) 2024/1624.
- Links between a virtual IBAN and a crypto-asset wallet. When a CASP (Crypto-Asset Service Provider) has an account with associated virtual IBANs, it can indeed assign these virtual IBANs to crypto-asset wallets. In such cases, the following data should be made available in the register of bank and similar accounts as part of the virtual IBAN referencing:
    - Data on the CASP
    - Country of establishment of the CASP
    - An indication that the virtual IBAN is associated with a wallet
    - Identification of the associated wallet
    - Data on the end-client (the CASP's client using the wallet associated with the virtual IBAN)

■ A specific format for vIBANs

The creation of a standardized format for virtual IBANs would facilitate their detection by various stakeholders in financial circuits (counterparties, financial institutions processing the flows, and the ultimate beneficiaries).

Responses to the ACPR questionnaire indicate that some institutions have assigned specific formats to vIBANs, such as allocating a particular bank code or branch code. However, these practices are not standardized.

The Bank of Italy has also observed among certain intermediaries the practice of using a specific branch code or inserting functional distinctive characters within the last 12 digits of the IBAN (the account number field) to make the virtual nature of the IBAN immediately identifiable—for example, the letters 'VA' or 'V' at the beginning of the account number field—thereby facilitating transaction monitoring.

Tracfin also notes that including the country of the redirection account within the vIBAN (for example, following the letters 'VA' or 'V'), as well as the bank code of the institution holding that account, could usefully complement this approach. Such a format would allow counterparties to account for geographical risk. If the bank code is included, this format would also simplify investigations by competent authorities. Instead of querying the country where the vIBAN was issued (which generally possesses only fragmented information), the competent authority could directly query the country where the master account is held and track the flow of funds more quickly and efficiently.

Differences in IBAN structures from one country to another could pose an obstacle to such an approach at the international level. Nevertheless, ACPR staff had discussions with the technical committee in charge of maintaining the ISO standard regarding a potential evolution of the standard to allow for the identification of the virtual IBAN, and potentially even the redirection country or institution.

2) Distinction between the classification as a virtual IBAN and that of a bank or payment account

The ACPR considers that the virtual IBAN service cannot be dissociated from the provision of a bank or payment account, and that only EU licensed PSPs (including through branches and agents) can issue and distribute EU vIBANs

Several situations should be distinguished:

Virtual IBANs in the form of accounts mergers (provided by the same establishment, under the same country code, and used by the same customer)

For several years, the ACPR had accepted the practice of 'virtual IBANs' provided that the examined IBANs displayed homogeneous characteristics of merged accounts: multiple accounts, each identified by an IBAN, are merged within a master account identified by its own IBAN and reflecting all transactions of the merged accounts. This analysis of virtual IBANs ensures compliance with funds transfer transparency regulations, which require that the account numbers of both the originator and the beneficiary be included in payment messages[14].

[14] Regulation (EU) 2023/1113 (information accompanying transfers of funds) specifies (Article 4.1) that "The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payer: (…) (b) the payer's payment account number". This prevents the payer from including any other number than the actual account number.

For an homogeneous account merger to take place, virtual IBANs should be provided by the same establishment, under the same country code, and used by the same customer as the bank or payment account used for recording transactions . Regarding other forms of virtual IBANs that do not meet these criteria, each IBAN may be analyzed as a standalone payment account maintained by the institution identified by the country code and the bank code of the IBAN.

This is not meant to prevent the customer from receiving or making payments on behalf of third parties, provided such customer is authorized to receive funds for third parties on his own account under applicable laws and regulations (e.g., as authorized under PSD).

Regulation (EU) 2024/1624 introduced the concept of 'vIBAN user.' This concept must be distinguished from two related concepts:

- The simple status of payer on the account: (a debtor is assigned a vIBAN in order to pay their creditor, who is a client of the vIBAN issuer). One distinction, for example, is that the vIBAN user would be the person for whom the payment redirected via the vIBAN is intended;
- The 'account holder': who receives the payment into their assets but intends the funds for the vIBAN user. There should be no situation where funds belong to a mere 'vIBAN user' in the absence of any account holder. Otherwise, the relevant account would not be subject to the full set of due diligence obligations that must be exercised toward customers, particularly regarding beneficial owners. The concept of the vIBAN user is complementary to that of the account holder but does not replace it. [15]

The concept of the vIBAN user is similar to that of the 'beneficial owner of transactions,' as defined in Article L. 561-2-2 2° of the French Monetary and Financial Code. Consequently, even before the application of Regulation (EU) 2024/1624, account-servicing institutions should already identify vIBAN users pursuant to Article L. 561-5 of the same Code: although this latter concept only targets natural persons, the identification of the intermediate legal entity remains necessary.

Certain forms of virtual IBANs should be considered standalone payment accounts

With regard to the characteristics of certain product marketed as vIBANs , the **ACPR analyses the provision of vIBANs managed by end-customers as their own account (Case 4) and the provision of vIBANs with a different country code (Cases 5) as an activity of providing payment accounts**. Such accounts would still qualify as vIBANs under the new EU framework mentioned above, if they have a redirection role (but not if they hold a balance, knowing that the same balance cannot be in two different countries at the same time).

Article 4.2 of Regulation 2023/1113 also states that "The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payee: (…) (b) the payee's payment account number".
The same rule applies for transfers within the Union in Art. 5, if accounts are used ("where all payment service providers involved in the payment chain are established in the Union, transfers of funds shall be accompanied by at least the payment account number of both the payer and the payee").
Art. 8 of Regulation (EU) 2023/1113 imposes on the PSP of the payee to address the case of transfers of funds lacking the required complete payer and payee information

[15] cf Banca d'italia et UIF *Indicazioni per i soggetti obbligati sull'applicazione degli obblighi in materia antiriciclaggio nell'apertura e gestione di conti di pagamento dotati di IBAN virtuali,* 12 December 2024, which also considers, like the ACPR, that a mere payer is not a beneficial owner of the transaction.

Article L. 314-1 I of the French Monetary and Financial Code (CMF), transposing Article 4(12) of the PSD2, defines a payment account as "an account held in the name of one or more persons, used for the purpose of executing payment transactions". Payment services (PS) are listed in II of the same article, reproducing Annex I of PSD2. Among the PS listed, SP3 c) provides for the execution of transfers associated with a payment account.

As illustrated in use cases 5a and 5b described above, vIBANs for which the country code differs from the country where the main account is held should be classified as payment accounts.

In the event of alignment with the country code of the main account, and as illustrated in the aforementioned use case 4, the classification as a vIBAN, as defined by the aforementioned Regulation (EU) 2024/1624, cannot be upheld when the services offered under the guise of virtual IBANs actually correspond to account-servicing activities. The provision of one or more of the following services to the holder or user of a vIBAN appears to provide indicators for considering this vIBAN as a standalone account:

- The issuance by the vIBAN issuer of documents linking the vIBAN to the name of a person other than the account holder whose identity has been verified by the institution;
- The issuance of an account statement or equivalent showing a balance, unless it is a simple sub-account of a standalone account held by the same institution for the same client;
- The initiation of payment transactions from the provided identifier to freely chosen third parties, including via application programming interfaces (APIs) (regardless of which originating account number appears in the payment messages);
- The execution of payment transactions to counterparties other than the holder of the account to which the funds are redirected;
- The execution of payment transactions between multiple identifiers provided by an institution to the same client

When virtual IBANs are classified as standalone bank or payment accounts based on the criteria described above, the procedures applied to them under other regulations (notably regarding seizures or requisitions) must be similar to those applied to French accounts, unless otherwise interpreted by the competent authorities in their respective fields. Consequently, the branch issuing the virtual IBANs is subject to the same obligations toward competent authorities as any institution offering payment accounts. The internal organization of the institution between its headquarters and its branches for account management cannot justify any extension of processing times, limitation of available data, or relaxation of the procedures implemented.

Additional observations may be made:

a. <u>An issuance of IBANs allowed under the freedom of establishment principle</u>

The provision of IBANs with a specific country code should only be possible for payment service providers that have an establishment (understood either as head office or branch), in the relevant country, in accordance with the freedom of establishment principle. This is actually due to the fact that national registers can technically attribute an interbank code, which is a key element of IBANs, to local establishments only.

As a consequence, an institution willing to offer an FR IBAN to its customers needs to open a French branch regulated under sectorial financial regulation (PSD2, EMD2, CRD, MIFID). This branch should be covered by the internal control procedures of the institution.

b. The French branch must be considered as servicing a payment account in France, to comply with the actual IBAN ISO standard.

In line with the IBAN ISO standard[16], a vIBAN like all IBANs points to the same account servicing financial institution and the Member State, where the account is actually maintained.

Therefore, **an IBAN should necessarily reflect the branch where the account is serviced**. Thus, French branches that issue IBANs with an FR country code should always be considered as legally servicing these accounts in France. In practice **branches legally servicing accounts should reflect customer money in their accounts** (including in their tax statements).

This does not prevent the branch to keep the funds at the head office (the liabilities towards customers in the branch's books are balanced with a claim on the head office). It is also possible that several tasks of the branch be outsourced to other locations (at headquarters for example), including book keeping, operations monitoring and IT, provided the branch is legally servicing the account and remains responsible for the activities that are outsourced.

Consequently, the financial flows operated thought French IBANs should comply with the local AML-CFT regulation and supervision. It is perfectly possible to have the accounts on the branch's book in full compliance with the ISO 13616-1 standard and at the same time be flexible as to where the accounts are actually serviced.

As described earlier in this document, the account at the French branch can work as a sweep account, where money moves automatically from the French account to an account abroad: such automated rules may have the same effect as virtual IBANs while ensuring compliance with laws and regulations. As mentioned earlier this is a high risk product from an AML/CFT perspective and requires that the French branch has a consolidated view of the operations of its customers, spanning across all IBANs, particularly in the context of its reporting and due diligence obligations.

c. Conditions required for a branch to passport in France

In the context of passporting, the ACPR addresses the risks of a virtual IBAN the following way:

- AML/CFT : The above-mentioned ML/TF risks mainly consist in the fact that a vIBAN obscures the geographic area in which the main account is located and may also mean that payment institutions are not complying with the applicable AML/CFT framework (i.e. from Host MS). For these reasons, the ACPR asks institutions notifying branches in view of obtaining French IBANs to i) **ensure that French AML.TF requirements are complied with** (esp. for KYC requirements and local presence of a AML officer) et ii) that **consumers be informed that French law applies**. Internal control procedures of the institution should address this risk.

- Consumer protection : in cases where the branch serves French consumers, ACPR asks institutions notifying branches in view of obtaining French IBANs to i) ensure that **French consumer protection** requirements (including recourse to French ombudsman) are taken into account et ii) that consumers

[16] The IBAN ISO standard (ISO 13616-1) defines an IBAN as an "expanded version of the basic bank account number (BBAN), intended for use internationally, which uniquely identifies an individual account at a specific financial institution, in a particular country".
A basic bank account number BBAN is an identifier that uniquely identifies an individual account at a specific financial institution in a particular country and which includes a bank identifier of the financial institution servicing that account.
A bank identifier is an "identifier that uniquely identifies the financial institution and, when appropriate, the branch of that financial institution servicing an account".

be informed that French law applies. Internal control procedures of the institution should address this risk.

- Clear identification of operations involving French customers: ACPR asks institutions notifying branches in view of obtaining French IBANs to always be **able to recreate, for reporting purposes, the exact perimeter of operations processed for customers using French IBANs** and to report it to ACPR.

- Technical clarification of accounts held by the institution: in order to have a clear views of payment flows and to avoid conflicts of laws, the ACPR refuses technical set-ups where several IBANs with different country codes are linked to a unique master account.

3) Management of AML-CFT risks associated with vIBANs by financial institutions

Following a joint analysis by the ACPR and Tracfin, and similarly to the analysis published in 2024 by the Bank of Italy, certain measures appear capable of mitigating the AML-CFT risks associated with virtual IBANs.

■ Implementation of procedures prior to the distribution of virtual IBANs

Prior to providing virtual IBANs and in accordance with the obligation to collect and update information regarding the purpose and nature of the business relationship—using enhanced measures for high-risk products (Articles L. 561-5-1 and L. 561-10-1 of the French Monetary and Financial Code)—the financial institution must ensure that the issuance of a virtual IBAN meets a clearly identified economic need and must document the intended use (cf. the various use cases presented in this report).

Based on a prior risk assessment of the vIBAN service implementation, and in accordance with Article L. 561-4-1 of the French Monetary and Financial Code and Article 2 of the Decree of January 6, 2021, relating to AML-CFT internal control systems, risk management and mitigation measures must be established. These may include, for example:

- Limiting the clients eligible for this service (PSPs or non-PSPs, corporate groups);
- Limiting the features offered (number of virtual IBANs per client, conditions for creating and deleting virtual IBANs, etc.);
- Restricting the use of virtual IBANs to incoming flows only;
- Or limiting the counterparties authorized to send or receive funds.

When the master account holder is a financial institution, including a crypto-asset service provider (CASP), and cross-border correspondent banking services as referred to in Article L. 561-10-3 of the French Monetary and Financial Code are offered, the account-servicing institution must comply with the obligations set forth in that article and in Article R. 561-21.[17]

In cases where correspondent services are provided within the European Economic Area (EEA), paragraph 13 of the ACPR sectoral application principles and paragraphs 8.18 and 8.19 of the EBA guidelines point out that a risk-based approach may require the application of certain due diligence measures related to cross-border correspondence: notably, collecting general information on the AML-CFT vigilance measures applied by the client financial institution to its own customer base, and ensuring that the client financial institution commits to providing data on its customers and their transactions upon request. The financial institution holding the account may also have a contractual

[17] See guidance published by the ACPR on Correspondent Banking (in French)

commitment to cooperate concretely and collaborate actively with the master account-servicing institution for AML-CFT purposes.

■ A reinforcement of transaction monitoring procedures

As stated by ACPR in its AML/CFT risk assessment[18], specific due diligence measures must be implemented. .

The use of vIBANs by clients must therefore be subject to monitoring that is proportionate to the risk associated with the client and the service provided (number of vIBANs associated with the master account, ability to receive payments from third parties, and the characteristics and location of the entities for which the vIBANs are requested).

Transaction monitoring for operations carried out via vIBANs should be based on an analysis of the overall activity of the master account, but also, separately, of each individual vIBAN, in order to verify consistency between the initially declared purpose and the actual use of the vIBANs. This vigilance must include the risks associated with the reassignment of vIBANs.

[18] ACPR, Sectoral Risk Analysis, June 2023, §2.2.1.9

Annex 1: Figures on number of vIBANs and volume of operations

- Number of virtual IBANs

The number of vIBANs is usually unlimited or faces only a technical limit (1,000,000 or 999,999),

On the basis of the reported, non-exhaustive figures, the average number of vIBANs used per customer is very heterogeneous. It is noted that on average only one vIBAN is allocated per individual, while the legal entities using vIBANs have multiple vIBANs attached to one single payment account: it is logically very high for FI customers (over 40,000 vIBANs per FI), much higher than for NFCs (33 vIBANs per customer).

- Volume of transfers though a vIBAN

In January 2023, the value of transactions carried out by virtual iBANs amounted to at least EUR4 billion, for 1.7 million vIBANs.

Kinds of customers	Number of clients using one or more vIBANs at the end of 2022	Total number of active vIBANs at the end of 2022	Transaction amount in January 2023 using a vIBAN
Financial institutions	18	731 004	664 967 608
Non-financial enterprises	18 458	610 669	3 283 552 371
Physical persons for non-professional purposes	372 832	387 280	49 395 657
Other : 1 association law 1901	1	117	2 681 737
Total	391 309	1 729 070	4 000 597 374

- Natural persons, main users of virtual IBANs

Although only 4 institutions offer such services to individuals for their non-professional needs, these ones are the main subscribers of vIBAN services, in terms of number (95%, i.e. 372,832 out of 391,309 at end-2022). Most of these customers rely primarily on the services of the same institution.

In the vast majority of the reported cases, using a vIBAN for retail flows allows the institution to offer services not provided by itself, namely SEPA network access (355,229 vIBANs) or, to a lesser extent, foreign bank identifiers (17,600 vIBANs).