11.12.2025

Newsletter – Fraud related to Virtual IBAN

Executive Summary

This edition highlights the growing misuse of Virtual IBAN (vIBAN) in fraud schemes and outlines practical measures financial intermediaries who are issuing vIBAN but also Financial Intermediaries processing payments to or from vIBAN can take to identify and mitigate the associated financial crime risks. As the use of vIBAN expands, particularly among international corporate clients, so do opportunities for exploitation by criminals leveraging regulatory blind spots and cross-border opacity. This Newsletter intends to raise the awareness on this typology of fraud and to outline best practices to financial intermediaries as they could be concerned without necessarily being aware.

What is a Virtual IBAN?

Virtual IBAN (vIBAN) is a rather new product that financial intermediaries around the globe have implemented in the past years. The popularity of this product is increasing as its very handy for international company groups to optimise their collection of payment flows and to improve their cash management. Unfortunately, this product is also misused for criminal purposes, notably fraud.

Compared to a “traditional” IBAN, a vIBAN is not an account itself but is an “alias” of a traditional IBAN, that respects the relevant ISO requirements and is linked to an account trough a reference number. This number is used as a reconciliation key that facilitates automatic reconciliation of payments and allocation of assets and as such it allows to streamline account structures, which is especially useful for corporate groups. As a practical example, an international leasing company can use vIBAN to collect payments from its customers all over the world in an efficient way.

Certain use cases that apply vIBAN, result in payments getting first executed in the domestic clearing system and subsequently forwarded / credited to an account in another country. This means practically that an account number starting with CH does not necessarily mean that the related payments are linked to an account in Switzerland. This technical specification is misused for criminal purposes as the use of vIBAN can create the wrong impression that the account receiving the payment is, for example, in Switzerland, whereas the vIBAN might be linked to an account in a country that is not subject to equivalent AML/CFT standards.

The reader of this newsletter has probably already made a payment to a virtual IBAN without being aware of it. However, this not necessarily suspicious as there are several very legitimate use cases for vIBAN. It highlights however that it's not immediately visible to the client of a financial intermediary or the financial intermediary itself, whether the payment is performed to a conventional bank account or to a vIBAN. These circumstances are misused by criminals to mislead a client in believing that he/she is performing a payment to a dedicated physical account in a given country. Therefore, this risk related to vIBAN do not only concern Financial Institutions issuing vIBAN but also all other financial intermediaries active in payment services.

Fraud Typologies Involving vIBAN

Unfortunately, the legitimate advantages of vIBAN are misused by criminals for various predicate crimes or money laundering. This newsletter focuses on the misuse of vIBAN for the purpose of fraud. The following table summarizes common fraud scenarios observed in the Swiss context where vIBAN were used to obscure the true location or identity of the receiving party:

#	Fraud Type	Modus Operandi	Role of vIBAN
1	**"Hi Mum" Scam**	Victim receives fake message from a pretended "child" abroad needing urgent funds. Often includes deepfake videos or voices.	vIBAN mimics the child's supposed location, reinforcing the scam's credibility.
2	**Inheritance Fraud**	Victim is told he/she inherited money from a distant relative and must pay fees to claim it.	vIBAN appears to belong to a legitimate bank in the expected jurisdiction.
3	**Invoice Redirection (BEC)**	Fraudsters impersonate vendors and send fake invoices to businesses.	vIBAN are disguised to match supplier formats, avoiding suspicion.
4	**Fake Investment Platforms**	Victims invest via fraudulent websites (e.g., crypto or forex).	vIBAN gives impression of a regulated, domestic financial institution.
5	**Romance Scam**	Online fraudster builds fake romantic relationships and requests financial help.	vIBAN aligns with the supposed location of the disguised partner (de facto, scammer) to build trust.
6	**Rental Deposit Scam**	Fraudsters advertise fake rental listings and demand upfront deposits.	vIBAN mimics a local landlord's account, making the scam seem legitimate.
7	**Fake Charity Scam**	Criminals pose as charities after humanitarian crises and solicit donations.	vIBAN appears to belong to a well-known local NGO or aid organization.

There are no reliable statistics concerning the percentage of fraud cases that are involving vIBAN. However, vIBAN is a rather new product and yet provided by all banks who are working in the field of Cash Management and Payment Services. Therefore, increased vigilance, monitoring and effective restrictions are very important for Financial Institutions offering this service or considering to offer it going forward.

Also, Financial Institutions who are not offering vIBAN shall verify whether their clients can be exposed to the negative use of vIBAN and enhance their tools accordingly as outlined in the best practices mentioned below.

Examples of simple fraud cases involving vIBAN:

- **"Hi mum" cases**

"Hi mum" scam cases are typically initiated trough messaging systems creating the impression that the child of a certain person, for example studying abroad, had its wallet and phone stolen. The alleged child contacts his/her family members via another phone number to solicit for help. Deepfake videos and deepfake voice are creating the impression that it's indeed the child studying abroad who is calling. The parents feel worried and want to help so they wire some money to the indicated account number. However, this account number is a vIBAN with the country code only apparently related to the country where the child is studying. As the vIBAN is misused, the payment flows are directed to the accounts of the criminals in third party countries.

In such scam cases, the victims usually identify the fraud too late as they are concerned by the need to help their children. As the story appears plausible and the account number indicated gives the impression of being related to a local bank, it does not create a suspicion until the parents get contacted by their actual children. Unfortunately, at that point, the payment has already been executed in many cases.

- **Inheritance scam cases**

Criminals are generating fake inheritance documents that are sent to the victim creating the impression that the victim has a far relative who passed away and that he/she is entitled to receive the inherited wealth. To extort some money from the victims, the criminals pretend that administrative fees are due to process the inheritance payments and request a payment to an account with a bank in the country of the alleged distant relative. A vIBAN is used for this flow and leads the victim to believe that the payment indeed goes to a domestic bank in the distant relative's country, as reported in the provided (fake) documents. However, as only the vIBAN must be indicated in the banking tool, the victims do not form any suspicion and wire the requested amount.

After the successful conclusion of the first payment, the criminals usually attempt to request for further payments alleging further taxes or other fees. Those additional requests usually lead to suspicions of fraud but at that point its unfortunately too late. The initial payment is already executed to a country that is not cooperative on financial crime matters, which makes the recovery of assets extremely difficult, if not impossible. The victim suffers a financial loss.

What are the best practices for Financial Intermediaries to consider when dealing with vIBAN?

While the use of vIBAN can have very legitimate reasons, especially for payment factories and corporates groups, it is also a product that can be exposed to increased financial crime risk, notably absent an appropriate risk management and control framework. This might lead to vIBAN being (mis)used to the purpose of obscuring the entities or countries effectively involved in the payment flow.

Overall best practices as to offering payment and collection business via financial intermediaries:

- Maintaining the integrity of the IBAN country code is a fundamental part of secure and efficient global payments, it supports, among others, correct routing, formatting and fraud and regulatory checks to be performed. Therefore, a country level vIBAN shall always be linked to, respectively require a payment account held in the same country as designated by the country code of the vIBAN (also covered in FATF R16).
- Financial Intermediaries shall not offer payment and collection services in which the intention to obscure a cross-border relation cannot be excluded, such as nested models across several parties with unclear intention.

Due Diligence on involved parties and usage of services:

- In the frame of the client due diligence, it needs to be ensured that the services of vIBAN are only provided to clients who have a legitimate use for vIBAN in the frame of their professional activity.
- Financial Intermediaries shall apply full KYC on third parties offering services to or only rely on KYC controls carried out by third party fully licensed and subject to a robust regulatory framework
- Implement a pre-approval process for vIBAN issuance, especially for clients in high-risk jurisdictions or in case the number of used vIBAN exceeds the expected nature of the business relationship and intended collection background. Furthermore, in 3rd party collection models, the financial intermediary providing a (v)IBAN to a 3rd party shall be able to block (v)IBAN without undue delay in case of a risk event.
- Include periodic review of vIBAN usage patterns to detect anomalies.

Transaction level controls and transparency:

- The holder of the payment account, i.e. the Financial Intermediary, is required to instruct / communicate to its clients to specify the Financial Intermediary as the beneficiary and account holder in the transaction. The 3rd party can be additionally mentioned to increase transparency of ultimate parties. However, the 3rd party should not be communicated as payee instead of the payment account holder. There are upcoming requirements in the UK and European Union addressing this risk related to Verification of Payee and Confirmation of Payee which will enforce controls to prevent 3rd parties from declaring themselves inappropriately as a payee

in the context of a vIBAN. Such requirements are expected to become industry standards and shall hence be considered.

- AML transaction monitoring tools shall be enriched to be able to implement the use of vIBAN into the set of parameters applied to the transaction monitoring to identify potential misuse of vIBAN. Transaction Monitoring tools could contain a method to not only screen the country code of the vIBAN but as well the BIC Code containing in the vIBAN. A discrepancy between the country code and the location of the bank holding the ultimate account could be flagged in the tool in case of mismatch or in case of a BIC code in a country exposed to high risk of money laundering.
- Furthermore, fraud detection tools shall be enriched to detect cases in which vIBAN are used. This could for example be displayed as a warning message in the e-banking application.

Financial Intermediaries shall have controls aimed at ensuring that either an underlying proof of sale and trade must be delivered to prove the legitimacy of underlying collection services, or in use cases without a possibility to prove sale & trade background – such as wallet-top-ups – a closed loop control is ensured allowing only pay-ins from preregistered and validated accounts. This shall be ensured by name-and-number-validations against the pre-registered accounts and account holder names.