Regulations, Compliance & Risk

- Regulatory and license impact on card issuing
- KYC and KYB requirements in card issuing
- Know Your Customer – in-house or outsourcing
- PCI DSS & other security requirements
- Reverse solicitation – marketing & promotion of card issuing in multiple countries

Regulatory and license impact on card issuing

Legal issues related to regulatory or payment scheme rules often arise in questions we receive from our partners and clients. In this article I would like to summarize key dependencies, limitations and rules that have a very important impact on payment accounts opening, card issuing and also acquiring or money transfer activities.

When you are launching a payment institution, you have several areas to cover. One of the most important of them is a legal and rules area. Usually this impact can be divided into three main groups of activities: legal requirements, anti-money laundering requirements (which is a specific type of legal requirements) and payment scheme rules. Let me deep dive into each of them.

Legal requirements

To operate payment activities, almost in any country you need to get a payment license. There are various types of payment licenses depending on the country, so here I would like to summarize the most important details. In many cases you can hear about EMI (Electronic Money Institution license), Bank (Banking license), Credit Institution, Acquiring Institution etc. These requirements are usually connected with operational activities that the company needs to fulfill to perform payment operations for other entities. They consist of:

- Regulatory requirements in the areas of security, Know Your Customer, AML, liquidity operations, organizational structure etc.
- Audits performed by regulator
- Risk of penalties for both the company and sometimes persons involved in payment companies
- Outsourcing activities compliance
- Local laws that forbid processing customer or transaction data outside of the country
- etc.

It is important to understand details of such requirements and to follow changes of law and rules on a regular basis.

From the business point of view those requirements force us to :

- Officially register contracts with various partners at the regulator
- Get an approval for particular actions outsourced to partners
- Perform regular monitoring of payment activities done with cards issued for users of our partners
- Follow the national and EU sanction lists

- Being ready to block any transaction, account or card at any time

For our partners - just make sure that you follow the rules we inform you about. They are critical for our activity, licenses, so in fact they are securing your business.

AML and KYC requirements

AML (Anti-Money Laundering) and KYC (Know Your Customers) are part of legal requirements but it is worth presenting them as a separate group because they usually have the biggest impact on operations. The main goal of these rules is to ensure that payment organizations are not used to launder money, support terrorist or illegal activities. They also allow governments to monitor a payment activity area which may be helpful in fighting crime activities.

Key areas of impact of those requirements can be summarized as follows:

- Payment institution is obliged to perform KYC requirements as defined by the regulator - usually consisting of collected proofs of user identity verification (documents, videos, selfie, talks, and other measures)
- In case of business customers and business accounts, not only Board Members but also Beneficiaries of the companies need to go through a KYC and sanction list screening. Beneficiary is defined usually as a person with above 25% shares
- At any moment a payment institution must be ready to present these documents to the regulator
- Persons and entities placed on sanction lists cannot use services of a payment company
- Active monitoring of payment transactions for all users is required
- Sometimes proofs of income can be required

It is interesting that AML and KYC requirements do not block us from issuing cards or opening payment accounts for partners located outside the European Union with our payment companies licensed in the European Union. We are allowed to perform payment activities for Brazil, US, China citizens, as well as the Polish, German or French ones.

Make sure that you collect user documents and provide them during the user registration to us to fulfill those requirements.

Payment Scheme requirements

Payment Schemes (Mastercard, VISA or others) have separate requirements that must be followed by their partners and licensees. These requirements are similar to the previous ones but not always the same. Key requirements that do have impact on business are:

- We are licensed for a particular country or region. In our case it is the European Union countries (in fact the European Economic Area, which is a slightly different area). It means that with our European licenses we can issue cards for people residing, having addresses or working in the European Union. In case we would like to issue cards for people or entities from outside the European Union we have to get special Mastercard approval which is not impossible but may be difficult to achieve.

- We must follow payment scheme requirements on sanction lists and scan users and beneficiaries against OFAC (US Office of Foreign Assets Control) and United Nations sanction lists.
- We must be ready to follow Mastercard technical and rules requirements that sometimes may have impact on technical setup and use cases of your users
- In case of mandates we need to be ready to implement on time necessary system updates to reach compliance with the Mastercard network

Problematic areas

Usually problems in a business discussion come in the following areas:

- Can we issue cards for non-EU citizens? Answer: generally yes, but sometimes there may be problems, the majority of your business must be in Europe, your user addresses or office should be in Europe etc.
- What documents do we need to transfer to you during registration? Answer: selfie, international passport is usually a minimum

Following regulatory, AML and payment scheme rules is critical for payment companies. We do not have a choice. This is part of the game of card issuing and we must follow requirements. However, it is good that such rules exist. They make our customers' money safer and minimize much bigger risks of running or supporting illegal activities.

Thanks for reading.

KYC and KYB requirements in card issuing

KYC (Know Your Customer) processes usually raise a lot of questions. In this article, I would like to summarize the most important decision points and requirements.

KYC regulations are directly connected with Anti-Money Laundering (AML), regulatory and sometimes with payment scheme requirements. In general, every payment or banking institution must be aware who its customers are, should know the source of its customers' funds, and should have information about the ways customers use money held by the payment institution. Regulators require that payment institutions know and monitor this in order to limit the risk of supporting terrorist or illegal actions.

The main question in every project is: "Who is the owner of the money on account?" We can have 2 situations:

1. CONSUMERS - If the consumer is an owner of the money on account, the KYC process has to happen. Usually it means that the user (consumer - not a company) needs to provide an ID document or passport and selfie, meeting or video call needs to happen to make sure that consumer is a real person signing a contract with a payment institution. There are various additional verification ways that a payment institution may require, but those are the key ones.

2. BUSINESSES - If a company is an owner of money, the KYB (Know Your Business) process has to happen. Usually it means that the user (company owner, manager etc.) not only needs to provide an ID document and make a selfie or a video call, but the payment institution needs to verify beneficiaries (the owners of more than 25% of shares in the company).

In both cases the payment institution is obliged to check whether the consumer, business manager or business owner is not present on various sanction lists, i.e. OFAC or UN sanction list.

These rules are critical and in fact all other implications are outcomes of them. In projects connected with launching Payout to Cards, the very first question that we need to answer is : "**Who is the owner of the money on account?**" If the consumer is an owner of the account (scenario 1) - the consumer needs to go through the KYC process. If the business is an owner of the money on account (scenario 2), the KYB process will have to happen and there will be no additional KYC.

There may be non-standard situations that will require some analysis. Let me present a few interesting scenarios:

- **Lendtech** - a company that provides loans to consumers. Let's imagine that this company is giving a loan of 1000 EUR to a consumer. We can have a project in two versions:
    - if the consumer receives a loan on his/her personal card - then we have the KYC requirement.
    - but if a card is just a part of Lendtech account and formally the consumer gets a loan at the moment he/she takes out money from the card account - we do not have any KYC requirement; we just need to do KYB for Lendtech. It can simplify user acquisition a lot.
- **Insurance** - an insurance company sends insurance value to users after a claim process or just after an accident:
    - if the user receives a gift card with 1000 EUR, which is the value of the claim, and at the moment of receiving the card, 1000 EUR on this card becomes his/her ownership - we have the KYC requirement for the user.
    - but if the user receives a card with a limit of 1000 EUR and when they pay - they use the insurer's money to cover costs of the claim, we do not have any KYC requirement. KYB will be enough for us.
- **Money transfer company** - let's imagine that the company sends a virtual card with 1000 EUR from Europe to the receiver in Singapore:
    - if the user receives a virtual gift card, and 1000 EUR belongs immediately to this user, we have to do KYC of this user
    - however, if users receive a virtual card with a limit of 1000 EUR and the money becomes theirs the moment they pay or withdraw funds from the card, KYB is sufficient. KYC is not required.

As you can see, there can be different approaches to KYC and KYB requirements, so it is worth reviewing the legal structure and thinking about how to improve the user experience in such projects.

Thanks for reading.

Know Your Customer – in-house or outsourcing

From time to time, our customers ask us whether it is better to perform **Know Your Customer** activities in-house or to hire a company to do it for them. In this article we would like to answer this question.

KYC activities are very important. **On-boarding** your customer is actually the first process that the customer uses, so smooth processes are critical for our future relationship with a particular customer. If the process does not work correctly, the customer can block and all our marketing and acquisition efforts will be useless. But how to do it right?

You can have 2 general scenarios:

Scenario 1 – build KYC in-house

You can start building this process yourself using **your IT team**. Actually, it is not so difficult. The process consists of a few **obligatory steps** that have to be performed by user:

1. Get user data
2. Get user photo or video
3. Get pictures of user’s document or documents
4. Check sanction lists
5. Approve / decline / get into interaction

It seems to be easy □□ but actually it is not so easy. There are some security and legal regulations that need to be fulfilled. There are specific requirements of payment institutions that will have to be fulfilled. You need to collect this knowledge, be ready to update your systems. Additionally, you have to think of automatizing this process on your side so that the user does not wait too long for approval of their application. From a financial perspective it sometimes can be much cheaper than automated KYC. Let’s do a quick calculation. If you hire a person and pay 10 EUR per hour to this person for performing KYC activities you can imagine that such a KYC employee will perform simple consumer KYC actions (verification of data, photos etc.) for one customer during 1 minute. It means that the cost of processing a single application is 10 EUR divided by 60 minutes = 0,16 eur per user!!!

Additionally, if you need to perform regular scanning of sanction lists, avoiding per user costs becomes more critical because there may be requirements that users are scanned against sanction lists once per month… If you have 0,1 eur cost per such scanning it means that you have variable cost of your operations. Very important disadvantage.

Advantages:

- Full control over the process
- Possibility of changing process in-house after product launch
- Full control over costs
- Possibility to avoid variable costs per user
- Possibility to avoid recurring costs per user
- Quicker responses to regulatory complaints as everything is in your system
- No dependency on external partners

Disadvantages:

- You need to spend time and energy on this process
- Time consuming process
- High fixed costs (team to develop and update the system)

Scenario 2 – outsource KYC

In this scenario you perform a tender and **choose the best KYC provider** for you. You can be quick with this process, you will get all technology this partner has but you will have to pay per user and maybe for some development and customizations. You will have an outsourcing company that most likely will have to be officially registered at your regulator as you are outsourcing anti-money laundering processes to this partner. It is definitely an easier process at the beginning of your journey but think about dependencies and cost.

In the long term you may also encounter problems with your partner that some specific requirements or unhappy path for your users does not work correctly. You should not think that you can automatize 100% of your on-boarding processes and you do not need to hire anyone. You must have some manual process, possibility to check application yourself and you must hold data yourself for future use.

From a financial perspective – you will have to pay per user or sometimes recurring fees per verification additionally. This may be a heavy cost for your business model. I think that this long term dependency is the critical disadvantage and you need to be careful.

Advantages:

- Quick time-to-market
- Professional processes achieved quickly

Disadvantages:

- High variable costs – clicks per user, monthly per user etc.
- Dependency on particular vendor
- Tendency to forget that you must have manual processes built together with such partner
- Risk of regulatory incompliance in case you do not monitor partner correctly

Summary

It is a difficult choice. In our opinion, in the short-term, it may be better to involve a 3rd party. However, in the long term, risk of dependencies, partner stability and variable fees seem important and you need to carefully consider if you do not want to have those capabilities in-house. Please also remember that while implementing 3rd party automatic solutions, you must have a manual process ready to process unusual customers.

Our services in this area are focused on this strategy. We use both 3rd party vendors and an internal system for managing KYC processes for ourselves and for our customers.

PCI DSS & other security requirements

Very often customers ask questions connected with security. In this article we would like to summarize key requirements connected with **Payment Card Industry Data Security Standards** (PCI DSS). There are other rules that we and our partners need to follow (like GDPR for example) but it will be the topic for another article.

The most important question that needs to be answered before going into details of PCI DSS requirements is - **Am I actually processing payment card data?**

Key PCI DSS requirements mentioned below apply only in case that the partner has access to card number (PAN - Primary Account Number), expiry data or other related card data. If the partner does not touch them, if the partner cannot see those numbers there is only one requirement - a simple Self Assessment Questionnaire (SAQ) needs to be fulfilled to confirm that the partner is compliant with PCI DSS requirements.

It is very important that you choose the correct way of integration with the card issuing platform. If you use our mobile SDKs or white label products, usually you will not have access to card data and will be able to approve your project just after fulfilling SAQ mentioned above. So please consider this way of integration to avoid additional costs and risks of PCI DSS compliance. However, if you connect via API, which is a usual way of integration, you will have to comply with security rules. Please read this section twice. **This is the most important** - choice of integration method will be decisive if you have to or not go through annual external audits and all hassle connected with PCI DSS.

Assuming you do process card data, depending on what your role is, different levels will be applied to you. You can be a **merchant** or a **service provider**. In simple terms, if you do the work for yourself then you are a **merchant** if you want to further provide the service (intermediary) you are most likely a **service provider**. In card issuing projects you will rather be a service provider because you offer cards to your users. Let me give some examples:

Service Provider - wallet, crypto wallet, money transfer organisation offering cards to own users etc.

Merchant - an insurance company that wants to use a card to send money to their users, a lending company that wants to send a card to users, a corporation or SME giving business payment cards to their employees etc.

Who is according to PCI DSS "Merchant"
PCI DSS, or the Payment Card Industry Data Security Standard, defines a merchant as any entity

that accepts payment cards (such as credit cards and debit cards) as a form of payment. The term "merchant" can encompass a wide range of businesses and organizations, including traditional retail stores, e-commerce websites, restaurants, hotels, and service providers that handle cardholder data.

Under PCI DSS, merchants are required to comply with a set of security standards and practices to protect the payment card data they handle. These security measures are designed to ensure the confidentiality and integrity of cardholder data, reduce the risk of data breaches, and protect both customers and the payment card industry as a whole.
PCI DSS compliance requirements can vary depending on the merchant's size and the volume of card transactions they process. Merchants are typically categorized into different levels based on their transaction volume, with higher-volume merchants facing more stringent compliance requirements.

There are 4 levels of compliance and requirements depending on volumes of cards and transactions.

Level of PCI DSS	Your business does	What you should do
4	· Less than 20 000 eCommerce transactions per year · Less than 1 million other transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
3	· 20 000 – 1 million transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
2	· 1-6 million transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) or ROC conducted by a QSA · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
1	· 6 million + transactions per year	· Complete an annual internal audit · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)

Who is according to PCI DSS "Service Provider"

According to the Payment Card Industry Data Security Standard (PCI DSS), a Service Provider is defined as any business or entity that is not a payment card brand (such as Visa or Mastercard) and is involved in the processing, storage, or transmission of payment card data on behalf of another organization. Service Providers play a crucial role in the payment card ecosystem, as they offer various services to help businesses accept and process card payments more effectively and securely.

Service Providers can include a wide range of businesses, such as:

1. Payment processors
2. Payment gateways
3. Hosting providers
4. Managed security service providers
5. Data storage companies
6. Point-of-sale (POS) system providers
7. Customer relationship management (CRM) software providers
8. Software-as-a-Service (SaaS) providers

Service providers are categorized based on the services they provide and their interactions with payment card data. Here are some common classifications of service providers based on PCI DSS:

Level of PCI DSS	Your business does	What you should do
2	· < 300 000 transactions per year	· Complete an annual Self-Assessment Questionnaire (SAQ) · Conduct quarterly network scans by an Approved Scanning Vendor (ASV)
1 (Verestro has 1 level of PCI DSS)	· > 300 000 transactions per year	· Complete annual internal audit conducted by a Qualified Security Assessor (QSA) · Conduct quarterly PCI ASV scans

Verestro has the 1st level Service Provider of PCI DSS, which means that we have to go through quarterly PCI ASV scans and an annual external audit performed by certified PCI DSS assessors. In accordance with the principles of PCI DSS, Verestro is obliged to check if the partner is working in compliance with the PCI rules, so we will be checking what the level of transactions and cards in your case is.

image-1713429427331.jpg

So let's remind our two possible scenarios:

Scenario 1 (The partner does not have any access to unencrypted PAN numbers) -> THIS IS THE BEST AND RECOMMENDED SCENARIO. In this scenario you will most likely use our SDKs and admin panel and full encryption of card data. Verestro will guide which Self-Assessment Questionnaire (SAQ A for merchants) is appropriate and ask a few questions (from SAQ). The document will have to be signed by the partner.

Scenario 2 (The partner can access unencrypted PAN numbers) -> in this scenario:

- Verestro will provide a Self-Assessment Questionnaire (SAQ), and ask a few questions. The document will have to be signed by the partner.

- The partner will perform quarterly PCI ASV (Approved Scanning Vendors) scans (cost around 1k EUR quarterly or less) - The partner can choose any provider from the PCI Security Standards Council (PCI SSC) or Verestro can recommend a supplier.
- Until the partner reaches 0,3 mln transactions/interactions annually with PAN numbers, the partner does not need to undergo an annual internal audit (in extreme situations, it is possible to require PCI internal audit from the partner).

If the partner plans to achieve 0,3 million transactions/interactions, there are two options:

- either the partner will move to a scenario that does not touch card numbers using some technology changes
- or the partner should perform an annual internal audit done by a PCI auditor (QSA)

If you would like to discuss your requirements in more detail and receive more information, please contact us.

Thanks for reading.

Reverse solicitation – marketing & promotion of card issuing in multiple countries

One of the limitations in **global card issuing** and **account opening** activities is connected with licenses and regulations for particular countries. Payment institutions have Mastercard or VISA licenses for particular countries as this is the way **Mastercard** and **VISA** systems work. In the European Union it is possible to get a license for the whole region but in other countries and regions you must get a license per country.

This makes the process of **card issuing** difficult in today's digital economy because you usually do promotional and marketing activities in multiple countries. You have users from Europe, Asia, Africa, Americas and other continents. It would not be smart to limit your payment services only to users from particular countries.

This is a critical point and you should be discussing this point with your **card issuer** at the beginning of your cooperation with them. The answer to this problem is not easy or white-black. There are some important considerations that we present below:

- **Multi card issuing and multi card processing** – we believe that integrations with multiple card issuers that have licenses in multiple countries is critical for the success of global programs. Verestro works with payment organizations in multiple countries and solves this problem globally. In such cases, those problems disappear.
- **Regulatory compliance** – your payment institution must check if it is legally possible to open a payment account and provide payment cards to users from many countries. In case of Quicko (our BIN sponsor) we are allowed to open payment instruments and accounts to users from multiple countries assuming we fulfill AML requirements
- **Mastercard and VISA rules** – Mastercard and VISA give licenses for particular countries. It is impossible to get a license for all countries. There are some specific processes to get approval for program in other countries than you have payment scheme license but it is not clear in fact and there are some risks for every program

There are some **general rules** that you should follow as our partner so let us describe it:

1. You should be able to prove that the main focus of your marketing actions is in Europe if your card issuer is based in the EU. We may ask some additional questions. Mastercard can have a look at places where transactions are happening etc. Try to focus on Europe.
2. You should be able to provide proof that even if we are distributing cards to consumers living abroad there is an economic interest of those people in Europe. Maybe they travel to Europe, maybe they have employees in Europe etc.
3. If you are distributing cards to companies, make sure they have headquarters or offices located and registered in Europe.
4. The best would be that your users have resident addresses in the European Union that they are registering during card on-boarding. This solves all the problems.
5. We would like to be aware of your marketing activities in countries outside of Europe. It is important that we are aware, maybe we inform local Mastercard so that they are aware.

Our intention in the long run is to solve this problem by working with multiple partners globally and grow with licenses to other countries together with our customers. Don’t hesitate to **contact us** if you want to do global card issuing business.

Enter section select mode