Flanks

flanks.io

Whitepaper

How does Flanks address security?

with Sergi Lao

Chief Information Security Officer and Co-Founder

The Open Banking Context

Since 2018, Open Banking initiatives have arisen across the globe, and clients want to be able to have a consolidated view of their wealth in the same place.

Although in Europe, the PSD2 regulation is limited to current accounts, the need to consolidate investment accounts is high. As for Latin America and the Middle East, the regulation is yet to come.

Open banking for wealth management is a recent but growing initiative. However, there is still a need to establish a global operating standard for sharing our clients' financial data. **To this day, a global, unified, and safe way of sharing financial data remains an unresolved challenge.**

As an AISP (Account Information Service Provider) company, Flanks always prioritises data confidentiality, integrity and availability. This implies ensuring our clients feel confident that their information is safe.

Flanks ensures that confidentiality, integrity and availability are our top priorities at all times.

For this reason, **we are interviewing Flanks´s main expert in cybersecurity, Sergi Lao, the company's Chief Information Security Officer and Co-Founder.**

This whitepaper aims to clarify any doubts or questions you may have about Flanks™ security standards, the processes behind our data gathering, and everything else related to them.

Sergi Lao
CISO and Co-Founder

1 Why is security important nowadays?

Today, cybersecurity is key in all sectors but especially critical in those that deal with sensitive data, such as health and finance.

Security must also coexist with the user experience, which is quite a challenge. Ensuring privacy, confidentiality, and data integrity must be one of the main objectives of companies in such industries. Financial services are highly regulated to uphold security, quality, and transparency standards.

2 What does Flanks do in terms of security?

Flanks apply protective measures in all data states (at rest, in transit and in use). We rely on physical security on quality and security certifications of Google Cloud Platform. Encryption standards are followed during all the communications on both external and internal communications.

Such methods of data encryption (known as RSA and AES-256) aren't customised but are part of well-tested and safe market standards.

Flanks is a SOC3, SOC2 Type II certified company that demonstrates our commitment to stringent control over data processing and security.

Finally, **we are also an AISP-regulated company, meaning the Bank of Spain validates our procedures and processes.** Besides, go through yearly audits by external companies like EY.

3 What is an Account Information Service Provider (AISP)?

An Account Information Service Provider is a company authorised to retrieve account data provided by banks and other financial institutions. It is a key player in the current Open Banking business environment and a core service that requires a **rigorous application process.**

The AISP license from the Bank of Spain provides us with the official authorisation required to access and process financial data securely, demonstrating our credibility and trustworthiness in the financial sector. Becoming an AISP allows a financial company like Flanks to compile data from multiple bank accounts. The AISP also explains to the end-user what data will be accessed, for how long, and who will have access to it. This digital consent journey forms the basis of data processing for AISPs under **GDPR.**

Moreover, being an AISP means we follow security standards and methodologies that we can apply to current accounts as well as other financial products. That way, it ensures that all processes are **audited, secured, and monitored.**

4 Where is data stored?

Flanks focuses on connecting financial data to any system. We offer the best flexibility for storing information, including the possibility of saving it in different models and regions. We can also limit or extend the scope of the saved data to guarantee its maximum privacy following GDPR's minimisation principle.

Flanks' solution is deployed in two different data storage models: It can be on-premise or as Software as a Service (in the Cloud). Both models obtain the data and credentials with the client´s consent. The extracted data and credentials are hosted in the client IT environment for the first one. Their IT team will take care of its security and the well-being of the solution itself, and the Flanks™ team will be available for any potential doubts. If you choose the second option, your data and credentials will be stored in Europe, in the Netherlands to be more specific. Flanks will be in charge of hosting, maintaining, and ensuring its safety. Flanks will also manage and secure your credentials, and both data and credentials will be encrypted and separated from the encryption keys.

5 How does everything translate into our day-to-day lives as clients?

As a regulated company, Flanks performs complete consent checks on every investor, advisor, and their respective e-banking accesses. Likewise, all the information about their past and present investments is encrypted from the beginning to the end. Concerning data confidentiality, within the scope of the GDPR, Flanks is a data processor. This means that Flanks does not share data with unauthorised third parties. Flanks complies with GDPR and acts on behalf of the credentials' owner, who gives their consent to retrieve and share the data extracted by Flanks with our client. The credentials travel directly to Flanks, following the best and well-known security standards, and the client obtains an identifier for them. Finally, the user **can request to remove the credentials from Flanks anytime and everything is wiped out.**

6 How do you access clients' wealth data?

At Flanks, we provide multiple ways to access clients' financial data, tailored to their preferences and the capabilities of their financial institutions.

For institutions that support structured data access, we utilise Power of Attorney (PoA), a secure and scalable method that enables automated data retrieval:

Flanks Credentials: with a PoA in place, the financial institution creates a dedicated, read-only online access for Flanks. This allows us to aggregate financial data independently, removing the need for client-provided credentials while ensuring secure and seamless data retrieval.

Data Feeds: also requiring a PoA, this method establishes a direct, structured data exchange between Flanks and the financial institution. Instead of relying on login-based access, the institution securely provides financial data files in a standardised format. This approach enhances automation accuracy and minimises client interaction. While the availability of Data Feeds depends on each institution's capabilities, they represent the most efficient and scalable way to aggregate wealth data.

7 Is any PoA data-access method better than others?

All methods ensure secure and reliable data access, but **Data Feeds** stand out as the most efficient and scalable option. They minimise client interaction by automating data retrieval, enhance security through institution-approved structured exchanges, and offer a frictionless user experience compared to credential-based access.

Additionally, financial institutions frequently favour Data Feeds, which streamline data management and make financial data aggregation more secure, efficient, and future-proof. While all remain solid alternatives, Data Feeds provide the best balance of security, convenience, and operational efficiency.

8 What if the client prefers an alternative to Power of Attorney?

Clients can use their own credentials as an alternative, in some cases, this option involves **Strong Customer Authentication (SCA) (also known as 2FA)** to access financial institutions securely. Unlike PoA, which requires a single client interaction at the start, client-owned credentials may require periodic authorisation from the client.

Flanks only triggers SCA when the user is actively present, avoiding unnecessary prompts and reducing the risk of unsafe habits like approving unknown notifications. We support multiple authentication methods, including SMS codes, phone calls, authenticator apps, biometrics, security keys, and QR codes, always following each custodian's security policies.

9 How does Flanks ensure my client´s credentials are secure if they use their own credentials?

Flanks stores access with a double encryption mechanism using Google Cloud´s KMS Service. Credentials are kept only with the user's consent, who accepts Flanks transferring the extracted data to the end client (financial advisor or an investment viewing application). Every credential-related operation Flanks manages is strictly monitored, registered, and read-only by default, and SCA **codes aren't stored anywhere.**

10 How do you ensure read-only access to the interface?

For regulatory reasons, financial entities require an SCA to perform any operation that directly and irreversibly impacts their financial situation, such as a wire transfer, buying stock, or shifting an investment fund. **Hence, the access granted to Flanks isn't enough to make an irreversible change within the account.** Likewise, the company is regulated and audited to reinforce the trust our users have in Flanks. We keep traceability of when and what type of data was extracted in all of our aggregations.

11 Isn´t a customer violating the T&Cs of the custody bank if they give their authentication data to a third party?

The customer wouldn't violate those, as GDPR is a higher standard than any internal policy. This means that although a financial entity may have policies or T&Cs against it, **the user has the right to share data with a third entity.**

Flanks follows **PSD2 and GDPR** regulations and has different binding legal opinion reports that validate the use of the tool at your disposal. Flanks simulates the behaviour of a web browser and limits bandwidth usage to prevent any disruption to the financial institution's website. Don't hesitate to reach out if any doubts or questions arise on this matter.

12 How can I start benefiting from Flanks?

You can reach us through our website's Contact page. There, you can schedule a first call with our Sales team in Spanish, English, French, or Portuguese if you have any doubts.

Our team will be happy to assist you and answer any questions you may have about your digital transformation.

Get in touch

Our wealth experts are here to help! If you have any questions or need more information, feel free to reach out.

Flanks

Wealth, easily managed

Let’s talk!

Flanks.io