WhitePaper

How does Flanks address security?

With Sergi Lao

Flanks

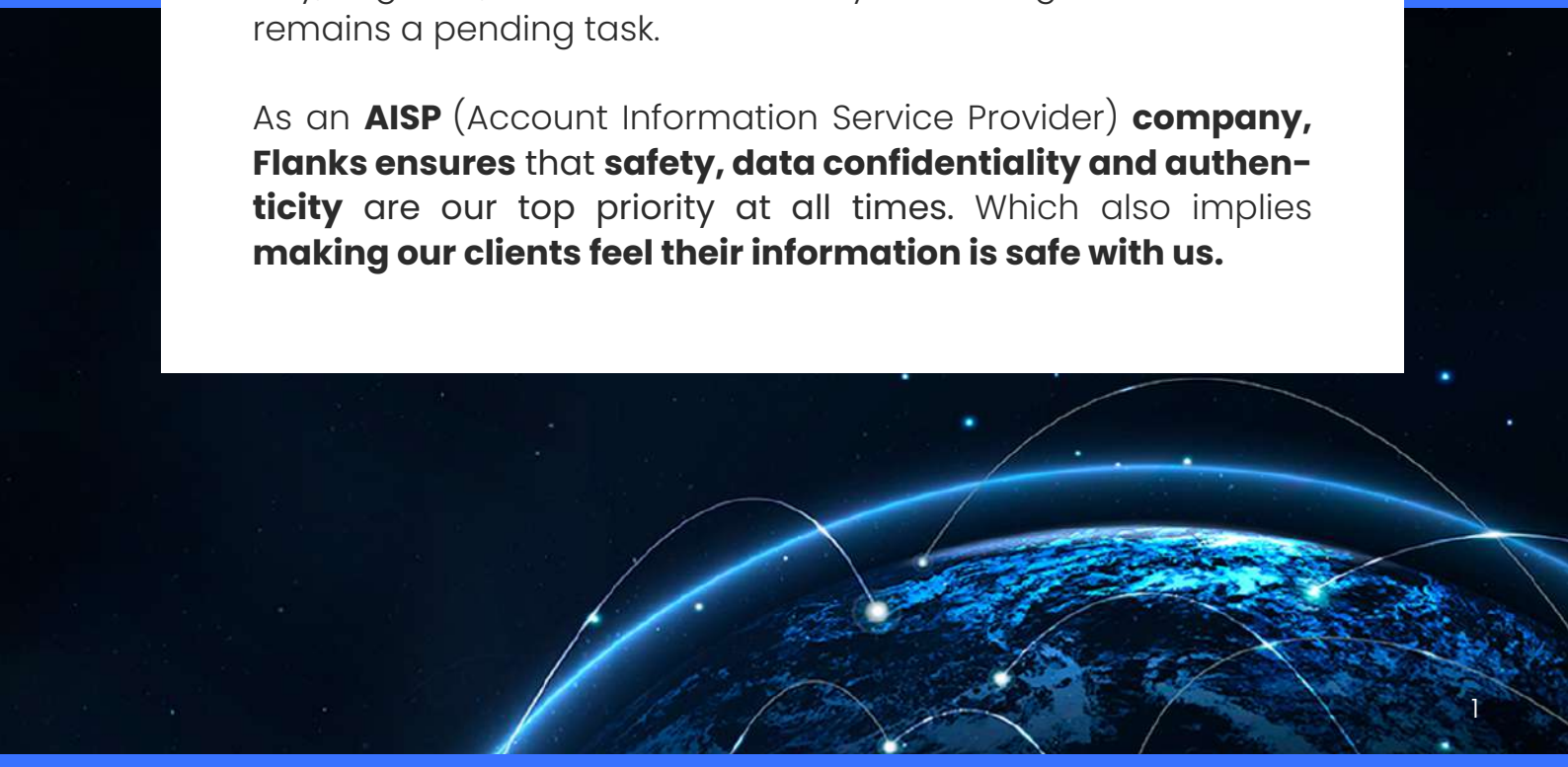
flanks.io | hello@flanks.io

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 finances with the same application.

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.

> Being open banking for wealth management a recent but growing initiative, there's still a need to establish a global operating standard to share the financial data of our clients. To this day, a global, unified and safe way of sharing financial data remains a pending task.
>
> As an **AISP** (Account Information Service Provider) **company, Flanks ensures** that **safety, data confidentiality and authenticity** are our top priority at all times. Which also implies **making our clients feel their information is safe with us.**



Flanks ensures that safety, data confidentiality and authenticity are our top priority at all times.

For this reason, today we are interviewing Flanks' main expert in security and cybersecurity: **Sergi Lao, CTO & CISO of the company.**

In this whitepaper, we expect to **help you break down any doubts or questions about Flanks' security standards**, the processes behind our data gathering and everything else in between.

1. Why is security important nowadays?

Sergi Lao: Today, cyber security is key in all sectors, but especially in those that deal with sensitive data, such as health and finances. Security is also something that has to coexist with the user experience, which is quite a challenge.

Ensuring privacy, confidentiality and data integrity (also known as CIA) must be one of the main objectives of companies in such industries. We should not forget that the financial sector is highly regulated, which seeks to guarantee an outstanding level of security, quality and transparency of services.

2. What does Flanks do in terms of "Security"?

Sergi Lao: Flanks protects data at all levels of the OSI stack (Open Systems Interconnection: The universal standard of communication functions in a computing system). We support the physical security of our infrastructure with the quality and security certifications of Google Cloud Platform. From the transport level upwards, security measures are followed, including encryption of both external and internal communications. Such methods of data extraction (known as RSA and AES-256) aren't customized but are part of well-tested and safe market standards.

Finally, we find it worth mentioning that we are an AISP-regulated company, meaning the Bank of Spain validates our procedures and processes. Besides, go through yearly audits by external companies like Deloitte.

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

Sergi Lao: An Account Information Service Provider is a company authorized to retrieve account data provided by banks and other financial institutions. It's a key actor in the current Open Banking business environment, and a core service that involves a rigorous application process.

Becoming an AISP allows a financial company like Flanks to compile data from multiple bank accounts. It's also the job of the AISP to explain 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, ensuring that all processes are audited, secured and monitored.

4. Where is data stored?

Sergi Lao: Flanks focuses on connecting financial data to any system, and we offer the best flexibility to store information. We offer the possibility to save it in different modes, nodes and regions. We can also limit or extend the scope of the saved data to guarantee its maximum privacy.

Flanks' solution is deployed in two different data storage models: On-premise or as Software as a Service (in the Cloud). In both models, the data and credentials are obtained with the client's consent.

For the first one, the extracted data and credentials are hosted in the client's IT environment. Their IT team will take care of its security and the well-being of the solution itself, and 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. Your credentials will also be managed and secured by Flanks, 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?

Sergi Lao: 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 very beginning to the end.

Concerning data confidentiality, within the scope of the GDPR, Flanks is a data processor. This means that Flanks does not analyze or share data with unauthorized third parties. Flanks complies with GDPR and acts on behalf of the owner of the credentials, who give their consent to retrieve and share the data extracted by Flanks with our client. The credentials travel directly to Flanks and the client obtains an identifier for these. Finally, the user can request to remove the credentials from Flanks at any time if they wish.

6. How do you deal with bank credentials having a 2-factor authentication login?

Sergi Lao: Flanks sees Strong Customer Authentication (SCA), also known as Two-Factor Authentication (2FA), as a safety asset for the users accessing their system. For this reason, it replicates the behavior a bank would have on the login process of each entity: If the bank sends an SMS code, Flanks will receive it and have visibility of the user's login process. We're aware that SCA can affect the user experience. That's why we work on having customized flows to collect the authorization from our clients in an optimized way.

Other than an SMS code, there are many more ways a user can go through a SCA: Through a phone call, an authenticator app using temporary secret keys, fingerprint and facial recognition, security keys, QR code... Flanks covers every method whilst following the security process of each custodian entity.

7. How do we retrieve the information?

Flanks uses an information extraction system of its own to ensure that every access is point-to-point encrypted. Its system doesn't only meet the main security standards but also replicates the security provided by the financial institution to be accessed (whether it's double biometric factor, SMS, token, etc.) Information is always extracted using both public and private APIs, providing an optimal level of security as third-party tools aren't needed for the access.

8. How do you encrypt the data?

Sergi Lao: Flanks stores accesses with a double encryption mechanism using Google Cloud's KMS Service. Credentials are given 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 operation managed by Flanks is read-only by default, and SCA tokens aren't stored anywhere.

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

For regulatory reasons, financial entities require an SCA to perform any operation that has a direct and irreversible impact on their financial situation. For example, 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 company. Likewise, the company is regulated and audited to reinforce the trust our users have in Flanks.

10. Isn't a customer violating the T&Cs of the custody bank if they give their authentication data to a third party?

Sergi Lao: The customer wouldn't be violating those, as GDPR is a standard higher than any internal policy. This means that, although a financial entity may have policies or T&Csagainst it, the user has the right to be able to share data with a third entity. Flanks has different binding legal opinion reports that validate the use of the tool at your disposal. Don't hesitate to reach out if any doubts or questions arise on this matter.

11. How can I start benefiting from Flanks?

Sergi Lao: You can reach us through our Contact page on our website. There, you will be able to schedule a first call with our Sales team in four different languages: Spanish, English, French and Portuguese. Our team will be happy to assist you and answer any questions you may have about your digital transformation.

Contact information

Our friendly advisors are always here to answer any questions you might have.

flanks.io/contact

hello@flanks.io

Faster, Safer and more reliable.

Flanks