Thales Gemalto
IdCloud Fraud Prevention
Flexible risk management for a safe and optimised digital banking experience
The challenge: Detect and prevent fraud while preserving user experience (UX)

With a multiplication of digital channels and massive adoption of mobile banking, financial institutions are facing a dramatic increase in the number of cyber-attacks. Phishing, account takeover and social engineering are just a few examples on how fraudsters and hackers constantly challenge security measures put in place. It is hard to stay ahead of cyber-criminals while maintaining a smooth user experience.

Yet, that is a must, convenience is key. Financial institutions must reduce friction for their customers and offer a convenient and secure digital banking experience, while making sure they comply with the latest security regulations, such as PSD2 in EU.

But that is not all. Today there are many technologies which can contribute to prevent fraud available on the market, making it a challenge to select, test, and integrate those that best meet the needs. In order to fight fraud efficiently and offer adapted authentication for their customers, financial institutions need expert guidance to assess their needs accurately. They need a flexible, scalable and future-proof risk management solution that let them efficiently monitor what happens on their digital channel in order to reduce fraud significantly.

And preventing fraud is not only about reducing financial losses, even more important is to keep your customers satisfied and secure.

Being in a reactive mode is very costly in terms of fraud losses and administration cost, but the worst part is the reputational damage which can be devastating and hard to recover from.

Enhanced risk assessment without frustrating your legitimate users

Gemalto IdCloud Fraud Prevention (IFP) is the risk management services at the heart of our cloud platform to secure and enhance onboarding and access to digital banking services. IFP allows financial institutions to assess every single online banking session in real time. It comes with selected pre-integrated advanced technologies to analyse a broad range of attributes from the user, device, network and transaction. Based on rules defined in the intuitive Policy Manager interface, the risk level of every single customer transaction is evaluated and the most appropriate authentication method recommended. This help to make the right choice to minimise fraud, either allow the transaction, block the transaction or challenge the customer with a step-up authentication. Thanks to IFP, financial institutions can define a granular authentication policy based on customer segmentation, customer preferences, use cases, and their own parameters. All running silently in the background to provide the best end user experience.

Thales Gemalto IdCloud Fraud Prevention

Flexible risk management for a safe and optimised digital banking experience

Banking & Payment Services

Scalable risk management for financial institutions to secure their digital channels and protect their users. It brings compliance to regulations, reduce operating costs and offer a smooth end user experience.
**Scalable and easy integration service**

IFP is a cloud-based solution, helping financial institutions to reduce their operations and fraud management costs by decreasing the number of alerts, claims and false positives.

As part of a scalable and open platform, it offers financial institutions the flexibility to include risk scoring from their existing risk assessment solution in addition to the best-in-class solutions that are already integrated, to get a single global risk score. The financial institutions can freely choose among the pre-integrated technologies and mix and match those that are most suitable for them. IFP brings peace of mind by gathering all services in one platform, removing the complexity of evaluating technologies and managing different suppliers.

The Policy Manager works on different use cases such as New Account Origination, login or payment. Based on the risk level of each use case you only involve the relevant fraud detection technologies to keep costs down and optimise total cost of ownership (TCO). When fraud patterns evolve over time the use case scenarios can be easily modified to always be one step ahead of fraudsters.

**A multitude of fraud prevention technologies**

There are five main technologies to fight fraud and IFP support them all; IP intelligence, device profiling, customer profiling, cyber threats detection and consortium intelligence.

With IP intelligence you detect suspicious network activities and locations. The capability to pierce proxies, understand TOR and VPN connections and identify geolocation from network information is mandatory in today’s fraud environment. Device profiling is used to determine if the device, which is used to perform a transaction, looks healthy and if the context around the transaction is normal. It also allows to recognise a returning device which is more trusted than a new device.

Customer profiling is all about understanding how your customer usually behaves, so you can spot unusual behaviour and raise suspicion, making it the most efficient way to fight social engineering fraud. As part of this, behavioural biometrics is used to passively gather data during actions the user is already performing, such as swiping, pressing keys or entering a PIN code. This is compared to previous sessions to validate the authenticity of a user. By checking transactional behaviour you can understand the user’s standard spending pattern to identify when a fraudster create an unusual transaction. Population profiling can also be used to compare one individual’s session behaviour with the collective behaviour of the population who have gone through the same flow, to spot irregularities.

The most direct way to detect a potential attack is to check for cyber threats. For instance if the device used is infected with malware this is a clear indicator that authentication should be stepped up or blocked. Using machine learning techniques it is even possible to detect yet unknown zero day malwares.

Consortium intelligence and sharing knowledge between stakeholders is one of the key defences since fraudsters often replicate their attack with different entities. The capacity to correlate multiple information such as email, device and phone number to build a digital identity which can then be associated with a reputation across the entire network makes your fraud detection stronger.

**Your trusted partner**

As the market leader in strong authentication and identity verification solutions we are a reliable and steady partner for banks and financial institutions that wants to launch large-scale projects. Our solutions already provide secure and convenient onboarding and access to digital banking services for hundreds of millions end users worldwide. Moreover, we are committed to support our customers in their continuous efforts on data security and data privacy.

**Benefits for financial institutions**

- **Optimise user experience**
  - Step-up authentication only when the level of risk is high
  - Benefit from frictionless Strong Customer Authentication (SCA)
  - Adapt authentication journey to customer profile
  - Runs silently in backend without disturbing user journey

- **Comply with regulations**
  - PSD2 RTS Article 2 on Transaction Monitoring
  - PSD2 RTS Article 18 on SCA exemption
  - FFIEC Appendix 5 Article 5B on Operation Risk Management
  - GDPR/CCPA compliancy on data privacy

- **Reduce operating costs**
  - One integration and contract to access multiple technologies
  - PSD2 RTS Article 14 on SCA exemption
  - Optimise usage of costly technologies to apply them only in relevant situations
  - SaaS solution reducing integration time and lead costs

- **Full visibility on digital channels**
  - Single consolidated dashboard to facilitate work of Fraud Manager
  - Detect fraudster strategy and optimise your policies in real time
  - Detailed statistics about your service usage
Comply with the latest security regulations

IFP is the perfect answer to new security requirements raised by regulations such as PSD2 and FFIEC. It offers real-time monitoring of the authentication and transaction process risk, as required in the RTS of PSD2. Complex security policies can be defined, based on the level of risk, the type of transaction and the user profile as recommended by FFIEC. It contributes to meet the requirement for stronger fraud prevention to fight against increasing attacks and fraud levels.

Data privacy regulations are becoming more stringent these days, especially with GDPR in Europe and CCPA in US. This can be a real challenge to comply with if data has to be processed by several different vendors for risk assessment. IFP has been designed for GDPR and CCPA compliance.

Thales Gemalto IdCloud
- a cloud platform to secure onboarding and access to digital banking

Our cloud-based managed services let financial institutions combine KYC, authentication and risk management services to secure onboarding and access to digital banking services and enhance the customer journey. With one simplified API.