IdCloud Fraud Prevention
Flexible risk management for an optimized digital banking experience

A scalable risk-assessment platform allowing banks to implement multi-layered security while offering a smooth user experience to their customers.
Banks’ challenges: Increase security and improve user convenience... with the right technologies!

With the multiplication of digital channels and the massive adoption of mobile banking, banks are facing a dramatic increase in the number of cyber-attacks. Fraudsters and hackers are constantly challenging the security measures put in place by banks to protect their customers’ sensitive data. Banks find it hard to stay ahead of the cyber-criminals while maintaining a smooth user experience... yet they have to! Convenience is key: According to a recent NIST survey, consumers are suffering from online security fatigue. They feel hopeless and overwhelmed being on constant alert for cyber-threats and are reluctant to deal with security. Banks need to limit friction for their customers and offer a convenient yet secure digital banking experience, while making sure they comply with the latest security regulations.

But that’s not all: Today, many different risk-assessment and fraud prevention offers are available on the market, making it more and more difficult for banks to select, test, and integrate the solutions that best meet their needs. In order to fight fraud efficiently while offering adapted authentication for their customers, banks need expert guidance to assess their needs accurately. They need a flexible, scalable and future-proof risk-assessment solution that allows them to reduce fraud significantly.

Enhance fraud prevention without frustrating your legitimate users with IdCloud Fraud Prevention

IdCloud Fraud Prevention (IFP) is a smart risk-assessment platform in the cloud that allows banks to assess every single online banking session in real-time. As a HUB, this platform comes with selected solutions integrated in it to analyze a broad range of attributes from the user and the device, such as geo-location, device profiling, IP address, device assessment and behavioral biometrics. Based on a set of rules defined in the Policy Manager, IFP evaluates the level of assurance banks should have for every single transaction performed by their customers and recommends the most appropriate authentication methods. IFP helps banks make the right choice to minimize fraud: allow the transaction, block the transaction or challenge the customer with a step-up authentication. Thanks to IFP, banks can define a granular authentication policy based on customer segmentation, customer preferences, use cases, and their own parameters.
Scalable and easy integration service
IdCloud Fraud Prevention is a cloud-based solution, offering broad and flexible authentication management based on multiple layers of real-time risk-assessment and enabling frictionless user experience. It helps banks to reduce their operations and fraud management costs by decreasing the number of alerts, claims and false positives.

As a scalable and open Hub, it offers banks the flexibility to easily integrate their own risk assessment solutions in addition to the best-in-class market solutions that are already integrated in it. IFP is being launched pre-integrated with Threatmetrix’s user and device identity network and with Behaviosec’s behavioral biometric solution. IFP brings peace of mind with one single platform, relieving banks from the complexity of evaluating technologies and managing different suppliers.

Behavioral biometric
IdCloud Fraud Prevention integrates in particular the analysis of behavioral biometric. Each person has a unique rhythm when interacting with a web page or a mobile device. Nobody can steal your ‘moves’ because they are largely second-nature behavior that is impossible to mimic. Behavioral biometrics uses measurable data created by user behavior to verify that the person using an account is the authorized individual. It gathers this data passively during the actions the user is already performing, such as swiping, pressing keys or entering a PIN code, and compares this to previous sessions. Within 7 to 10 sessions, the solution builds up a user profile and is able to evaluate consistency.

This behavior monitoring helps detect potential fraudsters in real time and contributes to the global risk assessment of IFP.

Comply with the latest security regulations
IFP is the perfect answer to new security requirements raised by new regulations such as PSD2 and FFIEC. IdCloud Fraud Prevention monitors in real-time the risk of the authentication and transaction process, as required in the RTS of PSD2. It enables banks to define complex security policies 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.

Gemalto is your trusted partner
The market leader in strong authentication solutions, Gemalto is a reliable and steady partner for banks and financial institutions that want to launch large-scale projects. Gemalto solutions already provide secure and convenient access to digital banking services to over 100 million end users worldwide. Moreover, Gemalto is committed to supporting its banking customers in their continuous efforts on data security and data privacy.

Benefits for banks

<table>
<thead>
<tr>
<th>Optimised user experience</th>
<th>Improved risk management</th>
<th>Compliance with regulations</th>
<th>Reduced operating costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differentiated user management</td>
<td>Multiple layers of assessment (device, location, user behavior, etc.) based on best-in-class solutions</td>
<td>Privacy by design compliance for data minimisation</td>
<td>Pre-integrated, flexible and future-proof solution</td>
</tr>
<tr>
<td>Silently running in background for frictionless security</td>
<td>Real-time assurance scoring</td>
<td>Cloud regulations compliant hosting facility</td>
<td>SaaS solution reducing integration lead-time and cost</td>
</tr>
<tr>
<td>More transactions accepted thanks to reduced false positives</td>
<td>Linked to proven step-up methods</td>
<td></td>
<td>Reduced number of alerts and claims to the fraud team</td>
</tr>
<tr>
<td></td>
<td>Integrating the bank existing scoring systems</td>
<td></td>
<td>Only use relevant technologies when needed to optimise TCO</td>
</tr>
</tbody>
</table>