NICE · ACTIMIZE

Preventing Fraud in the Open Banking Era

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Preventing Fraud in the Open Banking Era

Is the future of banking in open APIs?

Open Banking refers to a phenomenon in which consumers and businesses can execute payments and other services from their bank accounts via a mediator, also known as a Third Party Payment Provider (TPP), proxy, or aggregator depending on the service.

In this changing ecosystem of Open Banking, banks will provide a dedicated gateway, or API (Application Programing Interface), that exposes customers' data to the mediators, allowing them tobuild applications that interact with a bank's data. When the API's spec is shared freely it's known as an Open API or Public API.

Open Banking: A world of new opportunity … or concern?

Some believe that API-driven banking will give customers the freedom to do incredible things with their financial data, such as aggregating data from multiple cross-institution bank accounts to better manage their money. As importantly, banks may find new business models and revenue streams in Open Banking. In fact, some believe open banking models could eventually displace much of the traditional credit card business.

Yet the prospect is also terrifying for banks as a key question looms: Will they lose the grasp on their customers? Traditional banking products could become more commoditized if consumers latch onto third party services and mediators make it harder for banks to make decisions on transactions when the view of the customer is limited.

Open Banking as a Requirement

In Europe the market is already moving rapidly toward Open Banking, especially as the European Central Bank (ECB) published the PSD2 (Revised Payment Service Directive) regulation, which requires FIs to expose APIs and to allow third party providers to access customers' accounts. PSD2 rules aim to fuel competition in banks and FinTech, as well as to fight the card/plastic duopoly.

The UK has made great headway in the Open API banking arena, publishing Open Banking regulations, which focus mainly on data gathering and sharing to allow more institutions to better know the customer in order to offer competitive financial products.

Open Banking fraud and authentication concerns

Working in an Open Banking environment –poses a series of fraud and authentication challenges that must be tackled in order to secure this changing environment.

1. Fraud Risks: Open Banking can open the gate for new variants of fraud methods, including:

- **Account Take-Over (ATO) fraud on digital channels, 'flavoured' by Open Banking:** Open banking will open a world for many new TPPs and applications. As consumers get to know these new services, fraudsters will pretend to be TPPs, via rogue apps and phishing sites. Additionally there will be TPP data breaches, and fraudsters will then use this stolen data and credentials for account takeover in the traditional channels
- **ATO via the Open Banking channel:** Fraudsters will use stolen credentials via the Open Banking channel, to buy goods/ transfer money etc. While the TPP may be liable for such fraud, if the TPP uses the bank's authentication mechanism the liability might shift to the bank.
- **Customer Authorized Fraud (a.k.a. Social Engineering):** As with every financial service, consumers and businesses alike will be manipulated by fraudsters to make TPP transactions that appear to be valid. In Open Banking, however, things could be worse because customers will receive financial services and communications from multiple companies on top of their bank, leading to confusion and further vulnerabilities.
- **First Party Fraud:** As Open Banking aims to replace card services, we will see card-related fraud via this new channel (e.g. customers denying receiving the goods, loan fraud).
- **API Hacking:** In a sophisticated scenario, fraudsters may hack the APIs and utilize them (pretending to be a true TPP, or by hacking a true TPP and sending requests on its behalf).

2. Authentication Concerns: Open Banking raises multiple questions around authentication and liability. While regulations are not finalized yet, the most recent with regards to PSD2, determines that banks will need to allow TPPs to use the bank's authentication processes in order to authenticate the customer. This will have liability implications, but will also provide FIs more data on the customer for risk assessment. Banks are discussing how to expose authentication and how to manage the step-up process for transactions coming from Open Banking.

3. Operational Overhead: When it comes to fraud operations, banks will still be the natural address for customers when they suspect fraud in their accounts, and they will contact the bank Contact Center with queries, while the bank might not always have the right data and knowledge of how to handle that.

4. Technical Challenges: With Open Banking we can assume there will be a surge in transaction volume with multiple balance checks, automatic on-going access sessions and more requests from non-personal devices. Naturally this will mean a higher load on transaction monitoring and fraud systems.

How to protect your customers and your organization from fraud in an Open Banking environment?

Fraud protection for Open Banking operations should allow improving customer experience and providing greater customer choice, while protecting customers' data and limiting fraud losses.

Banks will be required to consider the following in order to detect and prevent fraud in an Open Banking channel:

- **Handle as a new channel while maintaining a cross channel view**
  Transaction leveraging Open Banking will contain new data that didn't exist in online or mobile channels (like TPP specific information). Some of the data used in the existing digital banking fraud solutions will be missing. So in their fraud controls banks need to consider Open Banking transactions as a new channel, leveraging the new data that comes with it and compensating for the "lost" data. This is true from the provisioning, account opening and authentication phases and through payments, loans and account services transactions. At the same time, banks must still maintain a customer-centric view based on activities in all channels.

- **Profile the new entities in the Open Banking environment**
  In their fraud controls, banks should carefully consider the new entities in this complex environment and relationships between these entities. Some analytics that were previously relevant when detecting card fraud will be relevant for protecting Open Banking transactions. For example, banks should profile TPPs and the relationship between Customer to TPP as well as customer's device to TPP.

- **Consider new dedicated risk indicators**
  In this new landscape, with new fraud threats, fraud analytics need to identify new risk indicators based on the new entities mentioned above. For example it can be useful to consider differently an existing TPP for a user vs. a new one, identify unusual activity from a TPP or a first activity from a rare TPP.

- **Prepare fraud operations for handling Open Banking**
  With the expected surge in transactions, customer confusion and fraud, banks fraud operations team can expect a high volume of cases to investigate and handle. In order to support this overload banks need to make sure they have the tools in place for efficient investigations and quicker resolution time.

- **Be ready for higher TPS and Big Data**
  Open Banking encourages competition and boosts the type of services consumers can get. So we expect that transactions volume will keep growing and their types will keep diversifying. Banks' fraud controls need to be able to deal with the new volumes, as well as variety and velocity.

Industry Trends

- Creating a channel - Banks are working to establish a proper Open Banking API channel, rather than receiving the mediators' traffic via the traditional channels (using for example screen scrapers).

- Regulation is still not finalized – Technical specs on the data items, liability, cashback and disputes are not finalized yet in Europe.

- FIs to leverage Open Banking – Bank may want to use Open Banking to get new data on customers, and come up with new products services and new business models, such as becoming sort of an "app-store" for their customers.