NICE · ACTIMIZE

PSD2

requires banks to enable customers to actively connect third party service to their bank accounts.

Are you prepared for PSD2 and its fraud and authentication implications?

info@niceactimize.com | www.niceactimize.com | www.niceactimize.com/blog

@nice_actimize | linkedin.com/company/actimize | facebook.com/NICEActimize

In the open banking era, transparency meets security with NICE Actimize.

Learn how we can help:

www.niceactimize.com/PSD2/FinancialIT

Financial IT

PREVENTING FRAUD IN THE OPEN BANKING ERA

With the European market moving at a rapid pace toward Open Banking, is this a world of opportunity or a cause for concern?

The European Central Bank's PSD2 (Revised Payment Service Directive) regulation, mandates the opening of the payments infrastructure to allow Third Party Payment Providers, or TPPs, to access banks' core banking platforms. PSD2 enforces competition in payments, allowing consumers and businesses to execute payments and other services via these mediators, but at the same time it also demands safety in providing such innovative services. The major concern is that Open Banking may very well open the gate for new variants of fraud at the same time.

The race to tomorrow – is the future of banking in open APIs?

Banks will provide a dedicated gateway, or API (Application Programing Interface), that exposes customers' data to the mediators, allowing them to build applications that interact with a bank's data. 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 commoditised if consumers latch onto third party services or the use of mediators could make it harder for banks to make decisions on transactions when the view of the customer is limited.

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. This new era of banking will no doubt 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 authorised 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) and API Hacking: In a sophisticated scenario, fraudsters may hack the APIs and utilize them (pretending to be

Omri Kletter

Head of Fraud & Authentications Solutions,
NICE Actimize EMEA

Omri Kletter is responsible for managing the fraud and authentication solutions in the EMEA region for NICE Actimize.

Prior to joining NICE Actimize, he joined the Security Division of NICE where he worked as the New Technologies Product Manager and was responsible for new initiatives including the division's Cloud and Cyber Intelligence activities. Mr. Kletter began his career in Israel's elite technological intelligence army unit, where he served as the Head of the Global Counter-Terrorism section.

a true TPP, or by hacking a true TPP and sending requests on its behalf).

Total fraud protection for the 'open channel'

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***
  Transactions leveraging Open Banking will contain new data that didn't exist in online or mobile channels (such as TPP specific information). Likewise, some of the data used in the existing digital banking fraud solutions will be missing. As a result, FIs need fraud controls which 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, FIs 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. We expect that transaction volume will keep growing and diversifying. FI fraud controls need to be able to deal with the new volumes, as well as variety and velocity.

Transparency meets security

Fraud protection for Open Banking operations should allow for improved customer experience and choice, while protecting data and limiting fraud losses.

It's important to strike the right balance with a fraud prevention solution that provides a winning outcome for both the banks and the customers they serve. The good news is that today's fraud solutions employ behaviour analytics that can very quickly spot unusual patterns indicating account manipulation and takeover. Additionally, open analytics technology can allow financial institutions to easily design their own fraud detection or risk models and stay ahead of emerging fraud threats.

NICE · ACTIMIZE