Onespan

https://www.onespan.com/blog/360-degree-view-how-customer-data-fuels-great-banking-experience

The 360 Degree View: How Customer Data Fuels a Great Banking Experience

Fraud Analysis - **Market Insights**
Benoit Grangé, September 9, 2021

In financial services, the digital channels have jumped to the top of the priority list, but the challenge of how to balance security and user experience remains. In the past, financial institutions (FIs) would increase security at the expense of the user experience, or vice-versa. That won't work in today's environment. Customers expect both a secure banking session and a satisfying user experience. They want to know that their bank is taking adequate steps to protect their life savings and personal data – without inconveniencing them every time they want to access their accounts.

The challenge is finding the right balance between security and a great customer experience. This cannot be achieved using traditional security and data analysis techniques. Historically banks would look at customer data, behavioral data, and the transaction itself to determine if a request was legitimate or potentially fraudulent. But they would only look at it by channel. Today's environment is multichannel or omnichannel, so that is insufficient.

To protect against today's complex fraud, FIs need to collectively harness their security technologies instead of operating them in siloes. That means bringing security technologies together in a hub, pooling the data, and flowing it to a risk engine to analyze. Taking a 360-degree view of all transaction and customer data across channels helps to identify anomalies associated with a transaction and determine when to request step-up authentication.

This approach is rooted in risk-based authentication. A 360-degree view of the customer leverages all available data points to create a user profile – taking into account customer data such as behavioral biometrics, passive biometrics, device characteristics, geolocation and transaction history. Then, with the help of its decision engine, the fraud prevention system uses a machine learning model to score the risk of each transaction. That risk score determines the next step in the authentication flow, which could be as simple as no authentication challenge at all for low-risk actions.

Let's take a closer look at how customer data can power a smooth and convenient digital banking experience, while also protecting against fraud.

Orchestrating Authentication Based on Risk

An in-depth data analysis benefits the customer experience because it equips FIs to dynamically adjust the authentication in real time. As an example, if François is transacting in Paris on the same smartphone he always uses and making a utility payment for the same amount he typically does each month, there is likely no need for any further authentication. However, if François is transacting online through a different browser than he usually uses, setting up a new beneficiary and attempting to make a payment of several thousand Euros, the fraud prevention system will present a high-risk authentication challenge (such as a facial scan) to François before processing the transaction.

This is foundational to designing the best possible customer experience. From the user's perspective, usual and low-risk actions will be smooth and easy – customers won't be bothered with cumbersome authentication. The goal is never to interrupt the user experience unless it is necessary. Customers should only be impacted when the level of risk justifies it.

This ability to adjust in real time reduces friction for the customer since the anti-fraud system is no longer applying a one-size-fits-all-approach. Instead, it makes decisions based on contextual customer data and adapts to each individual transaction.

Reducing False Positives

One of the most frustrating situations a legitimate customer can experience is being mistakenly flagged for fraud – and having their transaction cancelled or put on hold for manual review.

In the world of fraud prevention, one reason false positives happen is if the risk analysis is incomplete or incorrect due to insufficient data. False positives can also happen if the fraud system is working only with a data snapshot from the moment-in-time when the transaction took place, without considering the context around the entire banking session.

Financial institutions can reduce false positive rates by taking a 360-degree view of the customer. Leveraging all security tools in their stack enables FIs to collect a broad range of data points related to the customer, the devices they're using, their preferred channels, their accounts and the transaction itself – along with historical customer data and behavior patterns. With

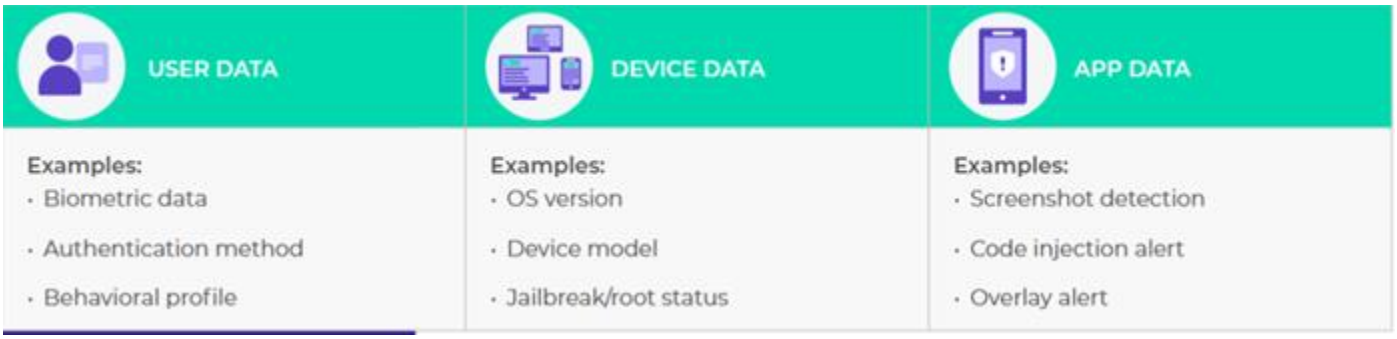
comprehensive risk analysis, fewer legitimate transactions will be labeled as potentially fraudulent, which in turn will translate into fewer requests for unnecessary authentication.

Mobile Data Drives Changes to the Digital Banking Experience

By leveraging the mobile channel to its full potential, financial institutions have access to much more data than ever before. That data can be used to better identify and stop fraud attacks in real time, while also improving the user experience.

In the mobile channel, financial institutions can gather real-time data on not only customers and transactions, but also about their behaviors, environment, location, biometrics and more. They can even use the phone's Bluetooth to discover other connected devices within the customer's proximity. All this data enables banks to gain deeper insights about their customers and meaningful context surrounding situations.

For example, a financial institution can learn exactly where the transaction is taking place — in the customer's home, or even from a suspicious location like a foreign country. Using the vast new volume of data made available by mobile, financial institutions can better understand each banking session and transaction in real time, enabling them to stop fraud before it happens simply by challenging the user with a higher-risk authentication method. If a fraudster is not able to then complete a facial scan, for example, the transaction can be denied or forwarded to the fraud team for investigation.



Examples of mobile-specific data collected to evaluate risk and adapt the authentication challenge

In addition to improving the digital banking experience, customer data can also help financial institutions respond to specific threats in an agile way by isolating customers at risk.

A good example is when a vulnerability is discovered in a mobile operating system, a situation that unfortunately occurs on a regular basis. Because the anti-fraud system will have previously collected data regarding what type of phone is being used by which customer, the bank can isolate customers impacted by the vulnerability – and can enforce an OS update, while all other customers continue to operate normally.

Closing Thoughts

Trust lies at the heart of the digital customer journey. Confidence in the financial institution's security is key to a positive customer experience, but FIs need to also balance security with convenience.

Risk analysis plays an important role in every aspect of the customer's digital journey. Without obtaining and processing enough device, application, transaction and customer data in real time, financial institutions cannot make informed decisions as to whether a specific transaction should be allowed, secured with an additional authentication challenge, or sent to the fraud analyst for a manual review.

Making the move to data-driven banking will require changing internal operations since siloed operations will need to share data. Ultimately, the goal is to harness your security tech stack to collect data and use the power of data analysis to turn raw customer data into information that you can use to both protect the customer and improve their experience.

The technology exists today to transform your banking operation to achieve this goal. OneSpan can help you get there.