Case Study: The Economics of User Friction in Digital Onboarding

How a change in liveness detection approach leads to a significant drop in abandonment rate and creates long-term value for financial institutions

This case review of a bank's transition of its customer onboarding technology illustrates how removing user friction is about more than convenience. Their upgrade from active to passive liveness detection demonstrates how removing friction can significantly decrease abandonment, and how that can hit the bottom line in a big way.

Measuring algorithm performance: biometric matching and liveness detection

Biometrics are playing an increasingly vital role in digital banking, enhancing remote identity verification and authentication security with biometric checks that complement other signals of fraud. Using facial recognition demands liveness detection to prevent bad actors from spoofing biometric comparisons with screens, photos, or masks.

The measurement of liveness algorithm performance is analogous to that of biometric matching. Both exhibit false-positive and false-negative errors, with an inherent tradeoff between security and convenience; the algorithms can be tuned to optimize for either. In matching, a false-positive rate indicates the frequency of incorrect matches between genuine and impostor samples, and represents a higher security threat. The false-negative rate points to rejections of genuine customers that negatively impacts user experience.

In liveness detection, APCER[1] is the rate of error in detecting a presentation attack, and liveness technology vendors tout a low or even near-zero APCER as a measure of the level of security it affords. But given the inherent tradeoff between false-negative and false-positive errors, a low APCER can come at the cost of a high BPCER[2], the error rate in classifying *bona fide* customers as legitimate.

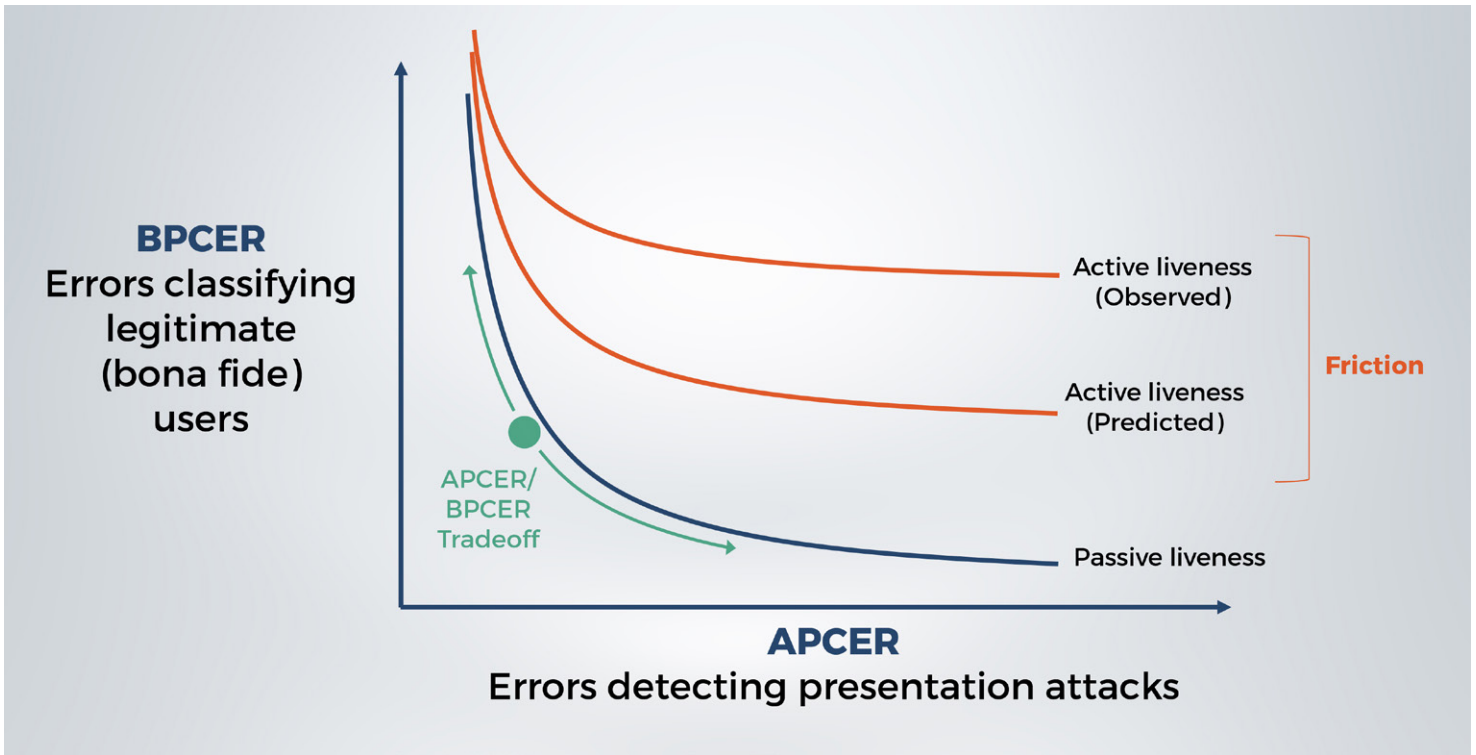## Friction contributes to a higher BPCER that is also less predictable

An "active" liveness detection approach relies upon interactions with the user to help assess liveness, while a "passive" approach is transparent to the user, and typically uses only the same images used for biometric comparison. A BPCER can be made worse by the friction introduced by an active liveness technique. Frustration, distraction, and errors in interpreting or executing upon instructions can all increase the frequency of interruptions and failures, and can be particularly impactful in a digital onboarding process, where users are new and performing tasks for the first time. Furthermore, user friction introduces variables of human behavior that are difficult to anticipate and measure, so the BPCER observed in a real-world deployment of a high-friction solution can be higher than planned for, and the difference can be significant.

[1]APCER is an acronym for Attack Presentation Classification Error Rate
[2]BPCER is an acronym for Bona Fide Classification Error Rate

Contact us at **info@idrnd.net** to learn more or scan the scan the code to visit **idrnd.ai.**

BPCER
Errors classifying legitimate (bona fide) users

APCER/
BPCER
Tradeoff

Active liveness (Observed)

Active liveness (Predicted)

Friction

Passive liveness

APCER
Errors detecting presentation attacks

Case study: the ROI from upgrading from active to passive, one-frame, frictionless liveness

A need to impose inconvenience on legitimate users (a high BPCER) in order to achieve a security target (a low APCER) can lead to abandoned applications and even lost customers. Case in point, an ID R&D partner with a large customer in the financial services sector had been using an active liveness detection solution. It had a low advertised APCER rate, but in the field they were experiencing a high rate of application interruptions; an observed BPCER in the range of 40%, which is astronomically high.

With only 60% of customers able to apply for an account without interruption, the impact on customer acquisition was substantial. So they opted to try a passive, frictionless approach as supported by ID R&D's IDLive® Face product. Unlike an active approach, IDLive Face uses only the same single selfie image used for biometric matching, adding zero effort to the user experience. Zero added effort means zero potential for user error contributed by liveness detection[3].

[3]An added benefit of a passive approach is that no information is provided to a fraudster on how to attempt to defeat it, which can lower the APCER.

From 60% to 95%+ completion rates for new applications

The results of the upgrade were dramatic. New customer applications went from a 60% completion rate to over a 95% rate. This means that over a third of all applicants went from being interrupted in their applications to completing them without interruption. The change was implemented without degrading spoof detection performance, i.e. without an increase in the APCER. Following is a more detailed account from the partner:

> *In real work operation, supporting millions of banking transactions a month, one of our customers migrated from an active face liveness technique to ID R&D passive liveness, and completion rates increased from 60% to 95%+. This was in one of the more challenging production environments with a very wide range of operating parameters.*

> *On the back of the improved liveness success rates experienced (faster, more accurate, much higher completion rates with many fewer attempts) the customer expanded their use of the system and their business dependency on ID R&D liveness for a much broader digital engagement on a long-term basis.*

The improvement was so substantial that it surely had not only a big impact on satisfaction across a broad swath of the customer base, but also on company financials. While not explicitly measured in this case, an increase in the rate of completions of over 50% likely had a comparable impact on customer acquisition and revenue.

Removing friction and reducing abandonments: the financial impact

Every prospective customer is valuable; but those who have already begun the onboarding process are particularly tragic to lose. We can estimate the value added by these customers who would have otherwise gone elsewhere. Consider an sample of one million account applications initiated both before and after the implementation of passive liveness detection. Without added friction from active liveness, 350,000 of these customers who experienced interruptions to their onboarding were now completing them without interruption. Even if only half of interrupted applicants abandon their applications altogether, we can estimate an increase in value to the bank in the range of about $350 to $700 million, assuming a retail banking customer lifetime value (CLV) of $2,000-$4,000[4] per customer.

Passive liveness can reduce BPCER, abandonments, and uncertainty

It's generally understood that with biometrics come an inherent tradeoff between false negatives and false positives that stakeholders need to factor in when designing a system. This particular case illustrates that in the case of liveness detection, a high BPCER rate can have a massive impact on completion rates, customer satisfaction, and ultimately the bottom line. The friction introduced by an active approach will tend to result in a higher BPCER for a given target APCER. Furthermore, the unpredictability of human behavior makes it difficult to extrapolate performance in a controlled setting to real-world operations. With each new banking customer adding thousands of dollars of value to a bank, the difference made by friction can have a big financial impact.

---

[4]https://novantas.com/wp-content/uploads/2013/10/Customer_Lifetime_Value.pdf