Facial Liveness Detection in ASEAN Banking

Advancing Security and Efficiency in eKYC

Facial liveness detection has emerged as a pivotal tool within the electronic Know Your Customer (eKYC) process in the ASEAN banking sector. This technology has not only aided in identity verification during user registration, but it has enhanced security for high-risk transactions. Innov8tif Solutions, a major player in the ASEAN eKYC landscape, contributes significantly to the adoption of this technology. This article delves into the imperative role of facial liveness detection within the ASEAN banking industry, shedding light on its significance, practical implementation, and its remarkable influence on fraud prevention.

The Ongoing Threat of Fraud

According to PwC, fraud prevention measures are working, but it is a stubborn problem. Identity fraud and trade-based money laundering are the top two financial crime typologies amongst ASEAN financial institutions, making up 67.9% and 50% of cases respectively.[1] Fraudulent fund transfers make up more than three-quarters of all fraud incidents, with 58% of financial institutions reported being victims. For large institutions (>US$10 billion revenue), 18% reported US$50 million or more in financial losses, while 22% of smaller companies (<US$100 million revenue) are hit with more than US $1 million in losses.[2]

The Crucial Role of eKYC and Facial Liveness Detection

As the ASEAN digital economy is projected to expand at an impressive 20-40% compound annual growth rate (CAGR), aiming to reach US$1 trillion by 2030, the adoption of advanced identity verification methods has become essential. EKYC processes, empowered by facial liveness detection, have gained prominence due to their role in enabling digital participation and ensuring secure cross-border remittances, online purchases, and access to digital government services.

In this digital revolution, the banking sector stands at the forefront, leading the way in adopting eKYC systems to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations. For example, in 2023, the Philippines Central Bank introduced amendments to existing customer due diligence requirements, including rules detailing how digital IDs can be used during customer onboarding. This adoption mitigates cyber-related fraud, improves user experiences, reduces reliance on manual processes, and offers valuable insights through digital consumer analytics.[3]

[1] Tackling financial crimes in ASEAN with Innovation technology and data - GBG

[2] PwC's Global Economic Crime and Fraud Survey 2022

[3] Philippines Central Bank Approves New e-KYC Rules - ComplyAdvantage

A Digital Shift

The mid-2010s marked the beginning of a digital transformation within ASEAN banks, resulting in the digitization of user onboarding processes. With a high regional mobile penetration rate of 75.6% (excluding Laos, Myanmar, and Timor-Leste) and over 400 million internet users, the region is embracing digitalization. Compounded with the rise of a digitally savvy generation, who are spending more than 6 hours a day on their phones has fueled the shift from physical to digital platforms. Despite contributing to only 5-10% of ASEAN's GDP, the demand for the digital economy continues to surge.

The regulatory environment has made it conducive for eKYC adoption, accelerated further by the pandemic. National government initiatives incentivize investments in the digital economy, especially across e-payments, e-commerce, and communication. Initially spearheaded by large international and regional banks, these initiatives have trickled down, resulting in a surge in demand for eKYC solutions, particularly among smaller localized banks.

Combatting Cybersecurity Risks and Fraud

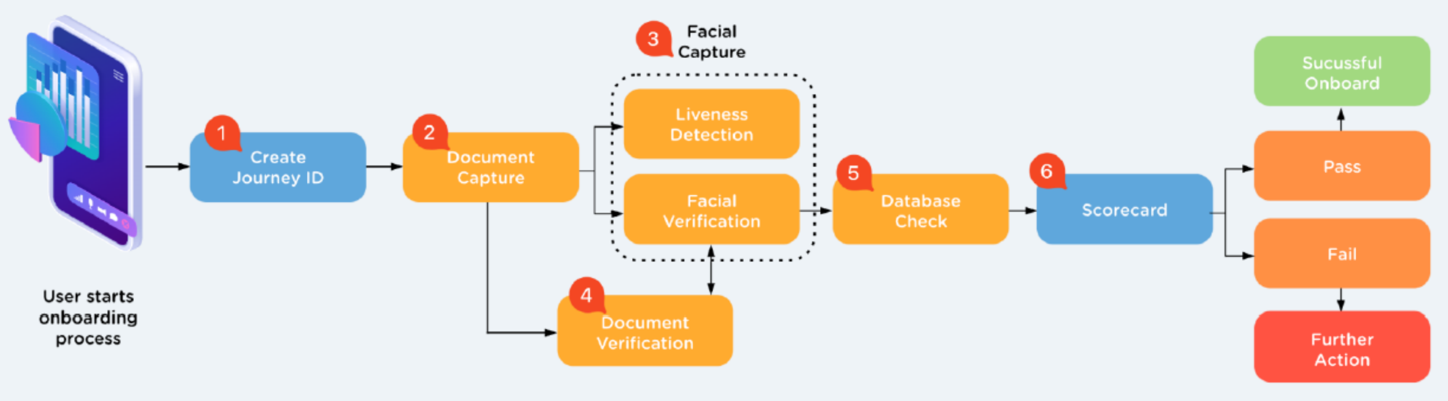
The rise in cybersecurity threats, exemplified by the growth of ransomware attacks, has prompted a reevaluation of security priorities. With a significant rise in ransomware incidents, banks are investing heavily in fraud prevention methods. Among these methods, eKYC incorporating facial liveness detection stands out. While fraudulent activities, such as identity fraud and trade-based money laundering, remain persistent, the implementation of liveness detection has resulted in a steady decline in fraud cases.

Innov8tif's Implementation and Impact

Innov8tif provides ID assurance solutions powered by artificial intelligence (AI) technologies, helping companies implement multi-factor authentication, automated customer onboarding, and customer due diligence systems. Their solutions are currently in use by public-listed financial institutions, telecommunications providers, and digital businesses across ASEAN member states.

EKYC implementations by Innov8tif has helped the ASEAN banks comply with KYC/AML regulations, reduced fraud rates, and deter fraud attempts. The solutions are designed to deliver a seamless user experience, capture useful analytics, and fully digitalize the user onboarding process. Their implementation of facial liveness detection follows a strategic sequence of steps:

1. **Unique Journey IDs are generated to track and store user signups.**
2. **Optical character recognition (OCR) technology automates the extraction of personal details from scanned ID documents.**
3. **Liveness detection, in the form of a live selfie, thwarts fraudulent tactics such as digital screen manipulation.**
4. **Facial recognition technology ensures alignment between the user's selfie and the photo on the ID card.**
5. **Rigorous checks authenticate the submitted ID document's legitimacy, guarding against forgery and other fraudulent attempts.**
6. **Cross-referencing against databases that include criminal records, politically exposed persons (PEPs), and suspicious signup attempts provides an additional layer of verification.**
7. **The system generates a scorecard that informs stakeholder decisions, offering insights and analytics through a user portal.**



The Role of Facial Liveness Detection in Fraud Prevention

Facial liveness detection plays a pivotal role in thwarting facial spoofing attacks — a type of cyber attack where attackers disguise their identity or impersonate others using digital screens or printed photos. The goal of such attacks is to deceive systems into believing that the attacker is a trusted entity, leading to potential security breaches or fraudulent activities.

According to Innov8tif's data, facial spoofing attacks have witnessed a significant overall increase, with a 110% surge from 2022 to 1H2023. Screen replays make up approximately 90% of these attacks, with printed copies making up the remaining 10%.

Interestingly, facial spoofing attacks occur at a higher rate in industries other than banking, and telecom in particular. A potential explanation is that stringent AML/KYC regulations serve as a strong deterrent to some fraudsters.

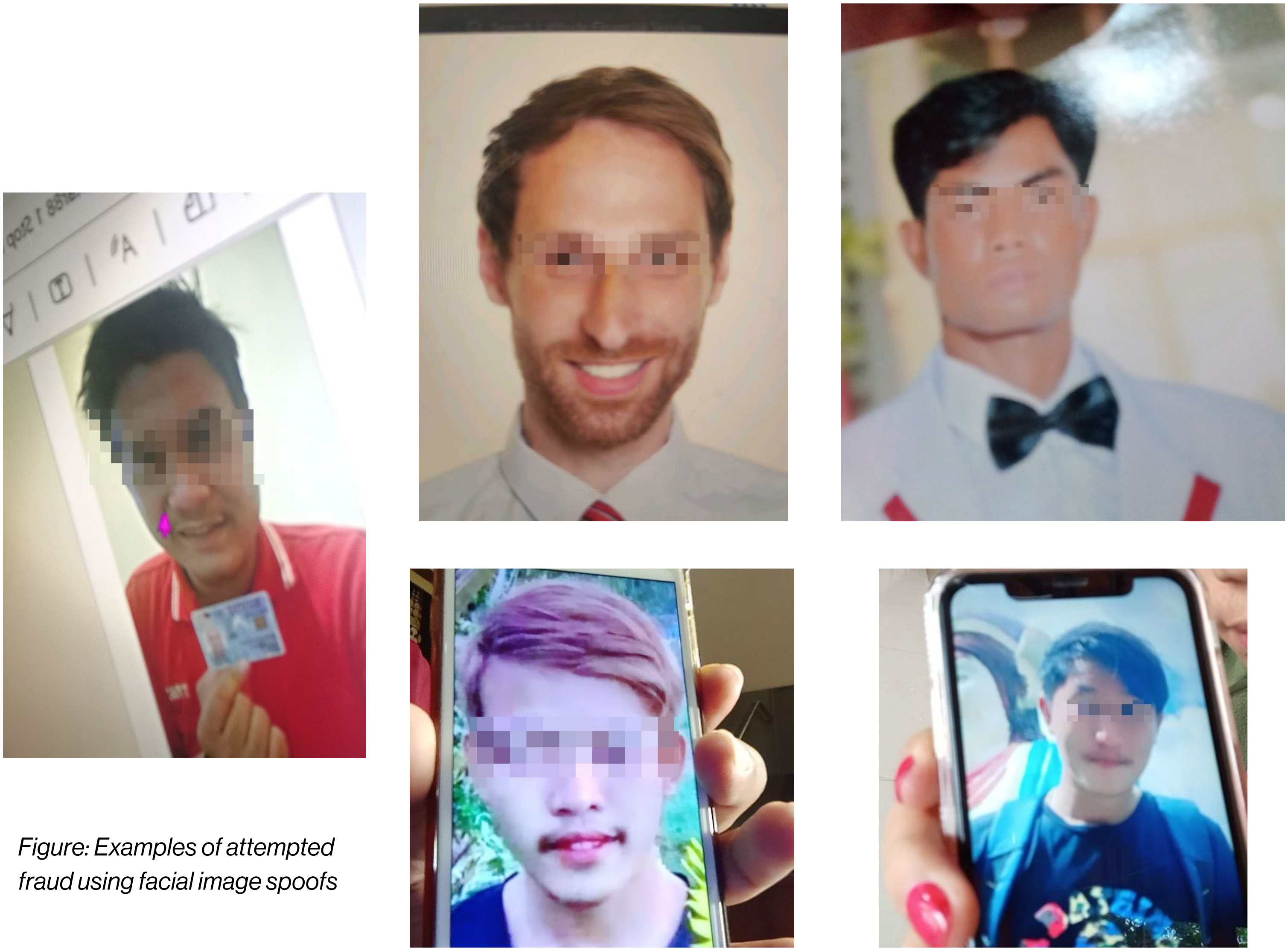


Figure: Examples of attempted fraud using facial image spoofs

Conclusion

Facial liveness detection is a cornerstone of the eKYC process in the ASEAN banking industry. Its integration strengthens fraud prevention, reinforces security measures, and fosters a seamless transition into the digital economy. With each thwarted spoofing attempt, ASEAN banks and Innov8tif contribute to authenticating accounts and safeguarding the legitimacy of digital identities. This technology not only protects consumers but also propels the ASEAN banking sector towards a secure and thriving digital ecosystem. - Joe Seah, Chief Commercial Officer, Innov8tif Solutions.

DISCLAIMER: ID R&D is not Innov8tif's sole provider of liveness detection technology. Innov8tif adopts a best-of-breed approach to adopting principal technologies for implementation projects.