

AI Company ComplyCube rolls out Face Authentication to fight fake signups and synthetic identities

The new service complements

ComplyCube's global KYC checks and

helps businesses implement strong biometric authentication to fight new identity fraud trends

LONDON, UK, June 21, 2022 /EINPresswire.com/ -- ComplyCube, the all-in-one verification platform, has rolled out [face authentication](#), bolstering its [biometric verification](#) capabilities.



Our award-winning adaptive AI platform continues to evolve to stay ahead of fraudsters and fight new sophisticated techniques employed by increasingly organized criminals."

*Harry Varatharasan, Chief
Data Scientist*

The new offering compares a client's facial and biometric characteristics to previously enrolled faces, allowing businesses to create strong authentication processes for gated services, account reactivations, and fend off Account Takeover (ATO) attacks, which have surged 148% across all sectors in the last 12 months.

The RegTech company has invested heavily in Research & Development (R&D) and Deep Learning models, in

particular, enabling it to roll out novel techniques to improve Presentation Attack Detection (PAD) and deepfake anti-spoofing technology in Q4 2021.

"With the introduction of Biometric Authentication, our award-winning adaptive AI platform continues to evolve to stay ahead of fraudsters and fight new sophisticated techniques employed by increasingly organized criminals", says Harry Varatharasan, Chief Data Scientist at ComplyCube. "Built on top of our core AI spoof detection engine, the new offering builds complex 3D face maps and scans highly optimized indices of banned faces to ensure only genuine customers get through" continues Harry Varatharasan.

The new service equips businesses with an additional security layer, which they can effortlessly deploy using ComplyCube's APIs and SDKs to protect themselves from emerging identity-based fraud trends such as organized fraud and synthetic identities.

1. Fake signups at scale

Criminals are increasingly flooding businesses with fake signup requests, typically by rotating faces across hundreds of attempts a day, using expertly crafted fake identity documents. Fake signups enable fraudsters to claim new account bonuses, cash drops, or create mule accounts. Organized gangs typically favor this type of fraud as they have the resources for large-scale operations. A higher number of attempts translates into a higher chance of success and provides a virtually guaranteed 'return on investment'.

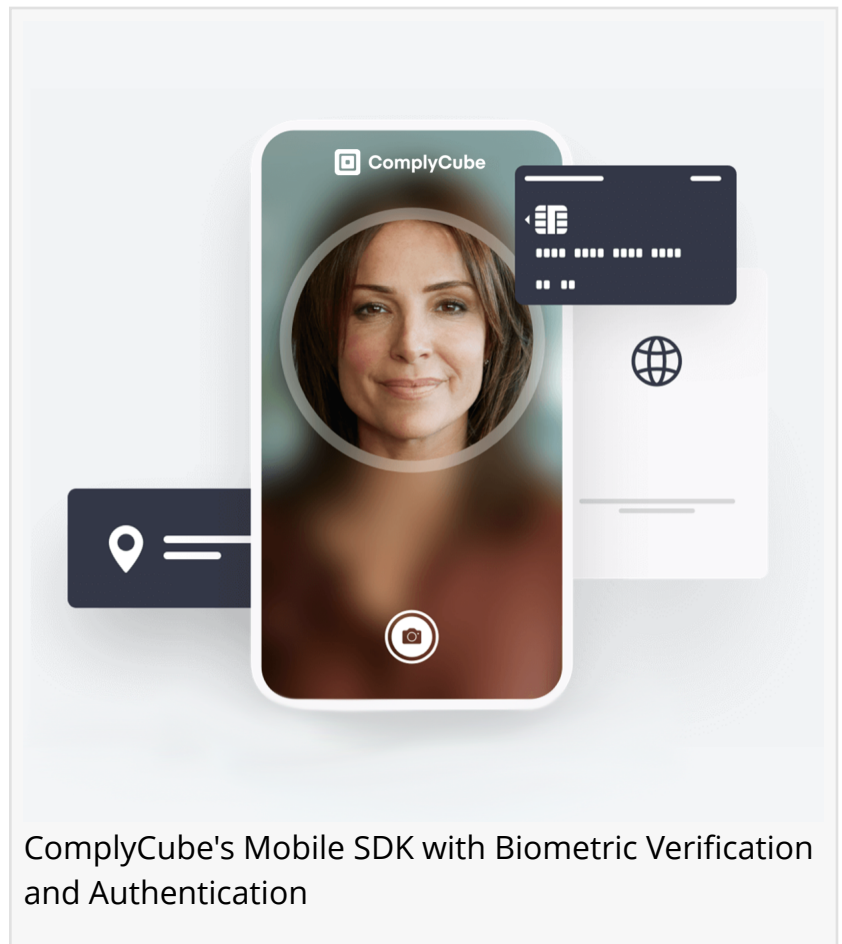
To prevent this type of fraud, a business must manually check identity documents and maintain a blacklist of faces previously used in fraudulent documents. ComplyCube's enrolled faces capability eliminates the need for such a manual process by screening at scale for duplicate faces used as part of onboarding. So, a fraudster attempting to open multiple accounts will be caught even if different personal information is provided.

2. Synthetic identities

Synthetic identity fraud is another troubling trend that continues to grow in sophistication, intensity, and frequency. Synthetic identity fraud occurs when an impostor combines real and fake personal information to create an identity and commit fraud. For instance, a fraudster may combine a stolen Social Security number (SSN) with a fake name, date of birth, and address to create a new identity.

The synthetic details, or the "Frankenstein IDs," are then used to apply for credit online. Credit bureaus typically reject the application because the synthetic identity has no credit history. However, the application alone means the crafted identity now has a credit file. Fraudsters then use this new synthetic ID to build good credit profiles, which may take months or years, and eventually, they "bust out," or borrow a lot of money and disappear.

This type of fraud is rising because stolen personal data is cheaper and more accessible than ever before. Nowadays, criminals are offering SSNs, full names, driver's license numbers,



ComplyCube's Mobile SDK with Biometric Verification and Authentication

passport numbers, and email addresses for as little as \$4. In other words, database checks, in which Personal Identifiable Information (PII) is checked against independent sources alone, cannot be an effective measure against fraud.

That's why businesses use ComplyCube's all-inclusive identity verification platform to complement database checks with additional anti-fraud layers of biometric and document checks, and ultimately have the best toolset for keeping identity theft at bay.

About

ComplyCube is a leading SaaS platform for automating Identity Verification (IDV), Anti-Money Laundering (AML), and [Know Your Customer \(KYC\)](#) compliance, with customers across telecoms, financial services, healthcare, e-commerce, crypto, FinTech, and more.

To learn more, visit www.complycube.com

Media Relations

ComplyCube

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/577632564>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 Newsmatics Inc. All Right Reserved.