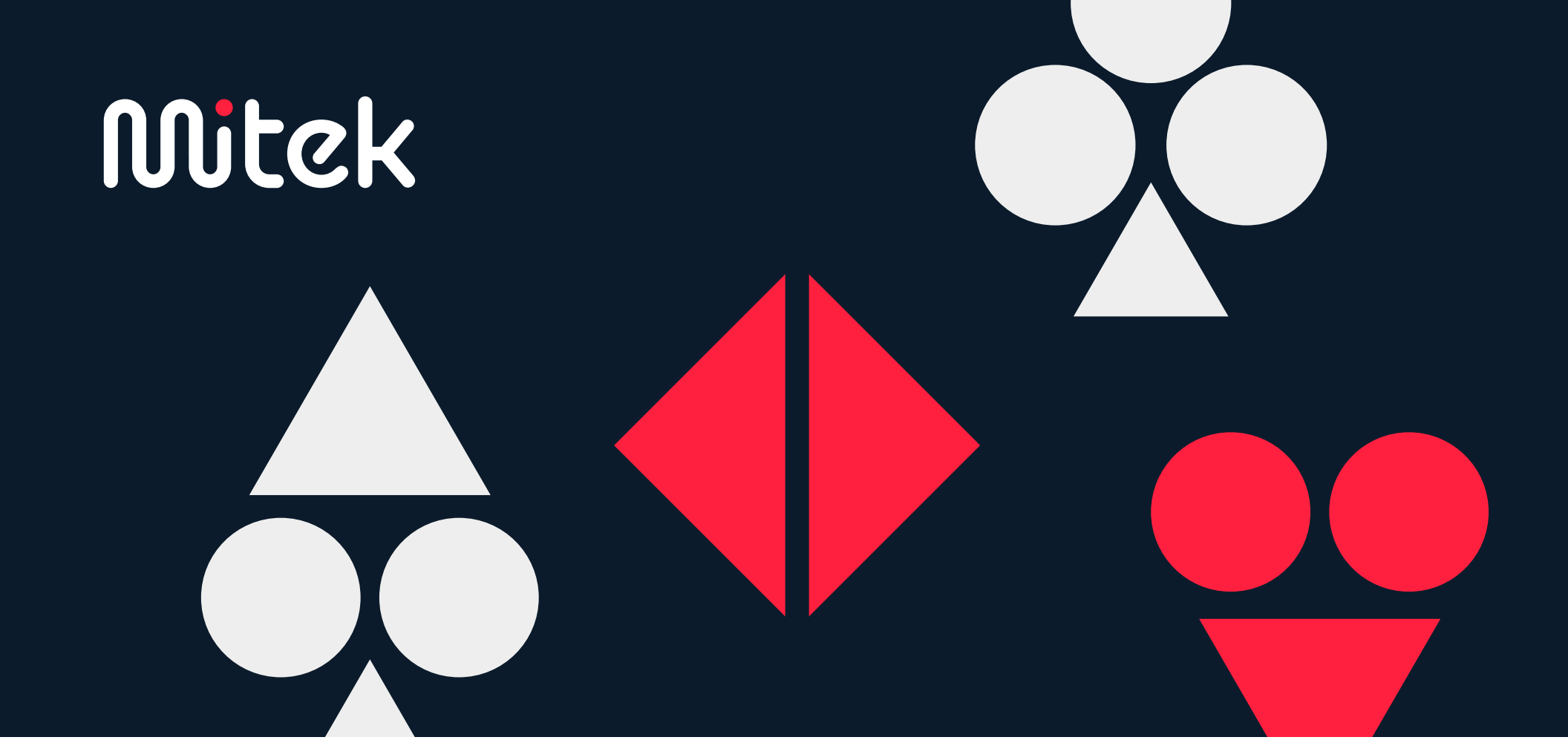


eBOOK:

BEATING THE ODDS

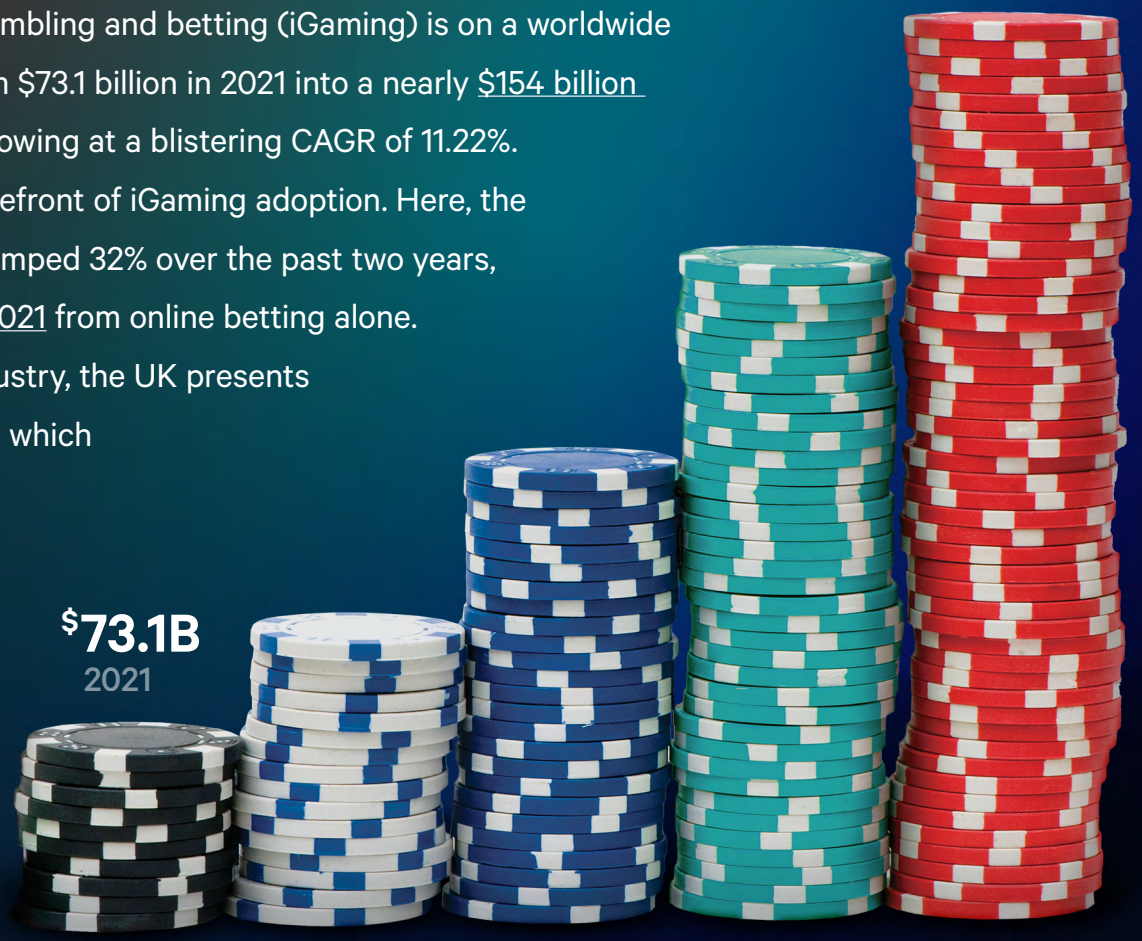
How iGaming operators and players both can win with facial and voice authentication

Where's the action? iGaming is a global juggernaut

In players' terms, online and mobile gambling and betting (iGaming) is on a worldwide hot streak. Forecasted to explode from $73.1 billion in 2021 into a nearly $154 billion global industry by 2028, iGaming is growing at a blistering CAGR of 11.22%.

The United Kingdom (UK) is at the forefront of iGaming adoption. Here, the number of iGaming participants has jumped 32% over the past two years, raking in $16.41 billion in revenues in 2021 from online betting alone.

As it has matured into a regulated industry, the UK presents a template for the US iGaming market, which generated $2.6 billion in 2021 and is growing at a CAGR of over 16%.



Regulation ignites iGaming growth

Government regulation is the driving force igniting the iGaming industry, and provides a roadmap to mainstream status for other once-taboo or illegal industries such as digital sex work and cannabis sales. While these alternative industries are a far cry from traditional financial services and fintech firms, they share identical challenges in protecting customers and themselves as they operate in the digital realm. iGaming operators in the US are additionally obliged to take action to safeguard customers under responsible gaming and self-exclusion regulations.

Fueled by unprecedented growth during the pandemic, the gaming industry is going all-in on iGaming to attract a new generation of customers, many of whom may never experience the adrenaline rush of brick-and-mortar casino wagering. A recent white paper published in the US by Casino.org reported that 36% of Gen Zers have placed bets only online and 48% of millennials have participated in online sports betting. Meanwhile, more than 70% of slot machine revenues in casinos come from players over the age of 55.

To ensure regulatory compliance, a strong identity verification (IDV) and age verification solution is a must. These capabilities go beyond regulatory call of duty, preventing fraud, money laundering, chargebacks and other financial crimes.

Best practices to beat the odds

This eBook shows how IDV is helping UK and US iGaming operators to comply with regulations, doubles down on IDV best practices, and explains how all firms can win against fraud by "betting with the house," by deploying a robust and flexible IDV platform.

GEN Z
36%
placed bets online

MILLENIALS
48%
participated in online sports betting

OVER 55
70%
casino slot machine revenues

iGAMING PLAYERS FIND THEIR ACTION

Sports and other betting
- Online sportsbook
- Fantasy sports leagues
- Team eSports
- Horse racing (online off track betting [OTB])
- Car racing

Gaming
- Online casinos
- Sweepstakes and contests
- Lotteries

Speculative investing
- Cryptocurrency trading
- Online trading communities

Operators are obligated to protect players – and themselves

Like any industry in which money changes hands, iGaming is susceptible to financial crime; during the pandemic, gaming fraud rose 393%. Regulations to deter financial crime vary widely by region, but across the board, adherence to them by iGaming operators is of paramount importance. Violations can result in major fines, trigger intense regulatory scrutiny of a wide range of related and unrelated processes and practices, and divert vast amounts of time and resources away from ongoing operations.

Players must be protected

iGaming players feel the most immediate sting of financial crime – gaming and bank accounts drained by hackers, identity information stolen by or unwittingly sold to fraudsters, financial peril from over-betting and more. The reputational fallout from regulatory lapses can be fierce, with players abandoning the offending operator and taking their business elsewhere.

In addition, underage iGaming has its own unique set of psychological risks. In the US, the legal age for gambling ranges from 18 to 21 depending on the state. But between 60% and 80% of US high school students report having gambled for money in the past year, according to the National Council on Problem Gambling. The group says the pandemic and easy access to online gambling raised the risks for these young adults, with 4% to 6% of high schoolers considered to be addicted to gambling.

For all of these reasons in the US, UK and around the world, iGaming operators are under extremely high pressure to meet regulations for identity verification and anti-money laundering.

In 2022 the owner of Ladbrokes was hit with the biggest fine in UK gambling history, a record **£17 million** ($20.6 million) for anti-money laundering (AML) and responsible gambling failures. About £14 million was due to failures at the group's online business, the United Kingdom Gambling Commission said.

Where's the fraud? Top types to beat

Account takeover (ATO)

Here, the fraudster gains access to the player's account by nefarious means – such as stealing login credentials, buying them on the Dark Web, hacking or other purposeful means – so they can withdraw funds to a different account. This can also be done by a fraudster setting up accounts for their own use with bought, stolen or "borrowed" legitimate identity information. Once taken over, the criminal can also deposit funds from the victim's bank account into the gaming account and withdraw them to their own.

Identity theft

Stolen identity information is readily available on the Dark Web. "Borrowed" identity information is obtained by fraudsters who pay victims directly to open iGaming accounts using their legitimate identity information. After the account is opened it is immediately handed over to the fraudster or money launderer.

Money laundering

iGaming accounts present a unique opportunity to introduce ill-gotten money into the legitimate banking system. Money launderers can deposit funds of illicit origin into their iGaming account to disguise it as legitimate winnings from online gaming. From there the funds can be transferred into the legitimate banking system.

Where’s the fraud? Top types to beat

Chargebacks

Criminal fraud occurs when a fraudster makes account transactions using stolen debit or credit card information, after which the victim files a chargeback claim. Friendly fraud is committed by the actual cardholder who, after playing a game, realizes they’ve lost too much money and contacts the bank to claim the charges were unauthorized.

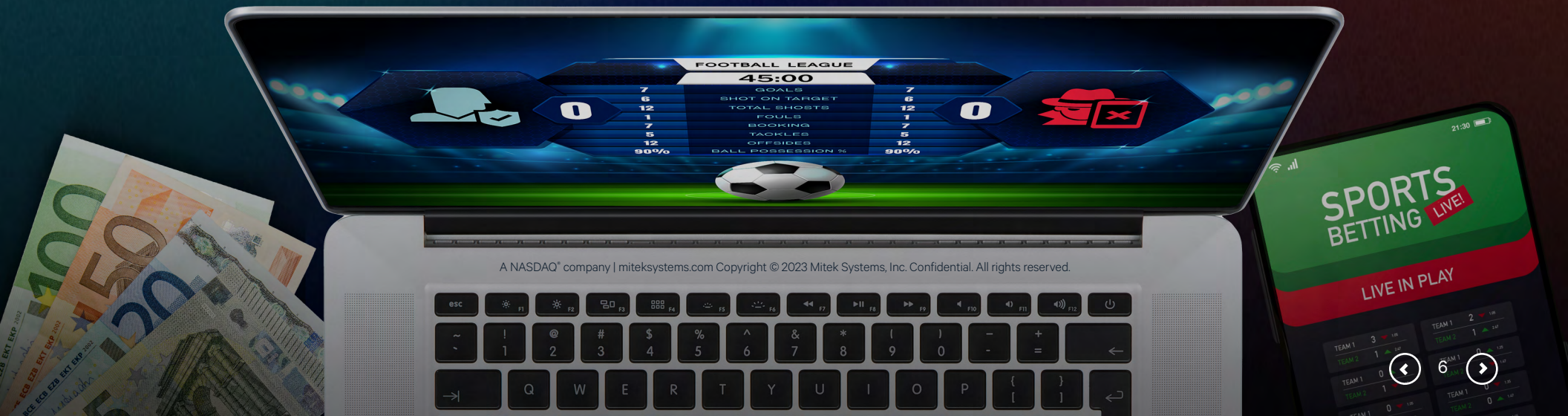
Arbitrage betting

Fraudsters place bets on all possible outcomes of an event in order to guarantee a profit, such as three bets on the outcome of a football match: one on each team plus one on a draw.

Multi-account abuse

A user registers several accounts to repeatedly benefit from free trials, and discounts, or to continue playing after getting banned. This includes chip dumping – making multiple accounts to play in the same game and deliberately losing to a designated account. Chip dumping is most common in poker and other card games.

Bonus fraud: A user registers multiple accounts to exploit welcome and bonus offers.



The IDV big three: Onboarding, fraud detection and AML

As in other financial relationships, identity verification typically occurs at the inception of a player's relationship with an iGaming operator. Across the UK, Europe and the US, IDV requirements vary widely; some jurisdictions allow wagers to be placed without verifying the player's identity. Other, such as Malta, require additional ID checks to be run after a player has spent €2,000 in a calendar month. Many jurisdictions' regulations open a window for criminal activity at account inception.

Safe, compliant iGaming requires IDV

To maximally fight fraud and financial crime, best practices point to frequent, fast and frictionless identity verification. An effective IDV platform can protect iGaming operators and players in three critical areas:

The IDV big three: Onboarding, fraud detection and AML cont.

ONBOARDING

Onboarding includes identity verification, age validation and data check (UK), known as know your customer (KYC) in the US. Identity and age verification confirm the player's name, age and address. This process typically involves the player submitting pictures of government-issued identity documents such as a passport, driving license or ID card. These are snapped with enhanced camera capabilities offered by the IDV provider's mobile app, which can be integrated into the iGaming operator's app. Address documents such as utility bills and bank statements can be used to further confirm name and address.

Some countries allow operators to enhance the onboarding process with other credible forms of data such as electoral roll data or credit data, the latter of which can be used to start building a player risk profile. Credit bureau data is available to licensed operators in the UK, for example, but not in other countries such as France, where privacy laws prohibit its disclosure.

FRAUD PREVENTION

Fraud prevention: Account takeover, chargebacks, multi-account betting and arbitrage betting can occur at any time. Fighting fraud requires integrating identity verification into critical processes to make sure that the player truly is who they say they are when:

- Placing a high-amount bet
- Placing a high volume of bets
- Requesting a withdrawal from the iGaming account to a player's bank account.

ANTI-MONEY LAUNDERING

Anti-money laundering: Money laundering is a global crime; once introduced into the legitimate banking system, funds can be wired nearly anywhere in seconds. AML precautions intensify the data check/KYC process by screening potential players against lists of people prohibited to become customers. To thwart money laundering iGaming operators use government-issued lists of politically exposed persons (PEPs), sanctioned individuals and entities, and global watch lists of persons, entities and countries identified as conducting or enabling terrorism, financial crime, the undermining of elections and human rights abuses.

The IDV big three: Onboarding, fraud detection and AML cont.

Widening the net on prohibited players

To further protect their business and legitimate customers, casino and iGaming operators screen potential customers against specialized lists from third-party providers, which can include:

- Persons affiliated with professional sports teams (athlete, coaches and staff); they are not permitted to bet on sportsbook games, a protection against game-fixing.
- Interdiction lists of people indicted for certain felonies such as financial crimes.
- People who are the subjects of certain types of negative news articles that may lead to legal punishment.
- An operator's own employees and management

iGaming and casino operators, like traditional financial institutions, are strictly forbidden from doing business with any prohibited customers.

Best practices in identity verification: integrated into customer journeys

Biometric authentication—the use of facial and voice recognition technology to gain access to iGaming apps and action—provides a trusted and secure way to authenticate iGaming players. With facial biometrics 10 times more secure, and voice biometrics five times more secure than traditional PINs, biometrics offer superior protection for both players and operators against ATO, identity theft and newer fraud types such as deepfakes and synthetic identities.

Face and voice authentication make the experience easy and frictionless

Invite

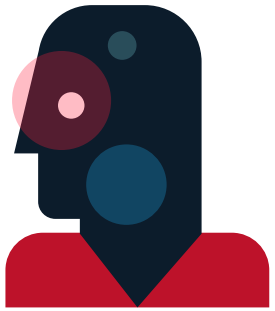
During the onboarding process, verified players are invited to enroll their face and/or voice biometric for trusted access to the iGaming platform.

Enroll

Players are guided through the process of taking a selfie and recording a passphrase, creating a baseline biometric template that is stored securely for future authentication.

Authenticate

Players can sign on with just a selfie or a provided passphrase. Artificial intelligence (AI)-trained algorithms and liveness checks help ensure the new selfie or phrase matches the stored biometric template to grant access within seconds.



Facial biometrics
10X MORE SECURE
THAN TRADITIONAL PINS

Voice biometrics
5X MORE SECURE
THAN TRADITIONAL PINS

Best practices in identity verification: integrated into customer journeys cont.

Frequent identification throughout customer journeys

The UK Gambling Commission's current advice to players is that "A gambling business may ask you for a selfie [for face authentication] if they think there may be fraudulent activity on your account." The reality is, iGaming presents a multitude of opportunities for fraudsters to insert themselves into legitimate players' customer journeys – the series of steps they take to accomplish key tasks such as creating an account with the iGaming operator, transferring funds into it, placing bets or wagers, and taking payouts.

Face and voice authentication can be easily integrated into these and other key customer journeys; simply put, biometric-based identity verification offers the highest level of security against evolving threats while delivering a superior player experience.

Payouts: Speed Matters

With payouts, verifying the player's identity at withdrawal can speed the funds' transfer while reducing risk. And speed matters. For example, research released in February 2023 found that **quick and easy payouts were prioritized** by 36% of players when choosing a sportsbook.

Payouts were more important than brand trust (34%), and odds and promotions (28% for both). Twenty-seven percent of players surveyed also said they also considered availability of preferred payment methods when choosing a sportsbook.

Battling the Bots

Industry reports estimate that more than **50% of traffic to iGaming and gaming websites comes from bad bots,** with fraudsters automating their attempts to cheat the system.

Facial and voice authentication can stop bad bots in their tracks, to thwart account takeover fraud, arbitrage betting, multi-account abuse, odds manipulation and more.

64% of customers trust biometrics more than passwords

- Source: Javelin 2021 Identity Fraud Study

An iGaming win: MiPass from Mitek IDV platform

The MiPass IDV solution allows operators to protect themselves and players from identity-based fraud and financial crimes. MiPass from Mitek strengthens operator trust in players' real-world identities using a sophisticated combination of biometrics that are extremely difficult to falsify: face, liveness detection and voice. For the first time, unsecure passwords and bothersome one-time passcodes can be replaced with facial and voice authentication that can be easily embedded into iGaming platforms and player experiences.

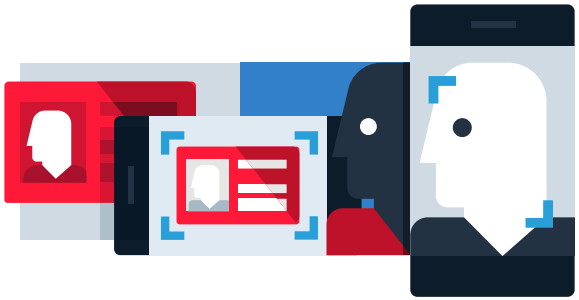
MiPass allows iGaming operators to verify the age and identity of digital players across the lifecycle of their gaming, starting with a frictionless onboarding experience and expedited data checks/KYC, continuing to ongoing AML compliance and fraud prevention.

A flexible, customizable cloud-based platform

Mitek's highly secure, cloud-based solution captures and stores encrypted biometric data securely – there's no sensitive data for iGaming operators to protect or manage. Biometric matching capabilities can be embedded into any player journey on the operator's iGaming app and are accessible from anywhere; there are no additional mobile apps for players to download or manage.

Mitek's developer-friendly software development kit (SDK) makes it simple to quickly embed and customize cloud-based biometric enrollment and authentication into a wide variety of iGaming use cases for onboarding, fraud prevention and AML. The MiPass platform can orchestrate "signals" (data inputs) from a wide variety of sources for situation-specific assessments. Business users can build specific customer journeys with Mitek's low-code/no-code development capabilities, picking and choosing from a wide range of signals including:

- Government identity verification and validation databases, including Department of Motor Vehicles (DMV) driving license data from all fifty US states, and across the UK and Europe
- Government and third-party PEPs, sanctions and other screening lists
- Facial and/or voice biometrics
- Liveness detection capabilities
- Geolocation information
- Fraud alerts
- Digital footprint analysis
- Behavioral biometrics (such as the way a user is holding, swiping or tapping on a mobile phone)
- Device identification and reputation



An iGaming win: MiPass from Mitek IDV platform cont.

Again, integrating IDV into customer journeys does not require IT developer resources; with the intuitive low-code/no-code MiPass interface, business users can graphically build them.

MiPass in action: ATO fraud prevention

- **The action:** Capture and enroll a biometric template during onboarding to use throughout the player lifecycle.
- **How it works:** During the initial onboarding process, Player Pete's identity is verified using a combination of ID document capture (is the document legitimate?) and live facial biometrics (is this the genuine owner of the document?).

The captured biometric is stored securely as a template. When Pete accesses his account in the future, places bets or other action, or requests a payout, a new selfie or voiceprint is compared against the stored template. If it's a match, Pete is authenticated and the good times roll. If someone other than Pete is trying to access his account, access is denied and the account is flagged.

What's next for iGaming and alternative industries?

With growth guided by regulation, iGaming is growing rapidly in the US, UK and Europe. In the US, at six states have legalized and regulated online gambling, with online poker and/or online casinos. Thirty-six states either offer, or are in the process of offering, online sports betting. Each state is responsible for enacting and enforcing its own iGaming regulations, creating formidable complexity for operators.

In the UK, iGaming has grown steadily since the enactment of the Gambling Act 2005. The uniformity of the UK's regulatory approach has catalyzed growth and provided a template for other regions to follow. However, in Europe, many countries have or are in the process of adopting their own regulations, after years of tax havens such as Gibraltar, Malta and Alderney (Channel Islands) allowing iGaming companies to be based those countries, near their main markets.

As iGaming growth continues its winning streak, identity verification with facial and voice authentication allows both operators and players to double down on safety, security and compliance. For more information about MiPass by Mitek iGaming solutions, visit miteksystems.com.

Learn how Mitek can help

Mitek (NASDAQ: MITK) is a global leader in digital access, founded to bridge the physical and digital worlds. Mitek's advanced identity verification technologies and global platform make digital access faster and more secure than ever, providing companies new levels of control, deployment ease and operation, while protecting the entire customer journey. Trusted by 99% of U.S. banks for mobile check deposits and 7,500 of the world's largest organizations, Mitek helps companies reduce risk and meet regulatory requirements. Learn more at www.miteksystems.com. Follow Mitek on LinkedIn, Twitter and YouTube, and read Mitek's latest blog posts here.

Learn more