Burbank.

Beyond the Odds.

Moving payment security for online gambling from prediction to proof

NOVEMBER 2026





6.8%

of global online gambling transactions were suspected digital fraud attempts in H1 2025

Source: TransUnion

+24%

increase in the volume of suspected digital fraud attempts in online gambling globally, H1 2024 - H1 2025

Source: TransUnion

14.2%

of new account creations in gaming and gambling were identified as attacks in 2025, up 68% year-on-year.

Source: LexisNexis Risk Solutions

Online gambling has a trust problem.

Online gambling has never been more accessible. Customers can create an account, deposit funds and start playing within minutes, from almost anywhere and on almost any device.

The shift from predominantly physical venues to a global, always-on digital market has transformed the industry. Customers now expect immediate access and seamless transactions, while operators have been able to reach new markets and engage players in ways that were previously impossible.

But as the industry has evolved, so too have the challenges of establishing trust in an environment where operators and customers may never meet. Behind every account, deposit and transaction is a fundamental question: *how can gambling platform operators be certain of who they are dealing with?*

This question goes well beyond payment fraud. Gambling operators need confidence that a player is who they claim to be, that they are old enough to gamble, that they are entitled to use the payment method attached to their account, and that each transaction is authorised by the cardholder.

The industry has responded with significant investment in technology, verification processes and fraud controls. Identity and age checks help establish who can open and use an account. Fraud detection systems analyse devices, behaviour and transaction data to identify suspicious activity, while payment authentication provides another layer of assurance. Each serves an important purpose, helping operators manage risk, meet regulatory obligations and protect legitimate customers.

But online, many of these controls are still trying to establish remotely something that is much easier to prove when the person, their payment card and their credentials are physically present. And the challenge is becoming harder. Suspected digital fraud in online gambling is increasing, while attacks at account creation show that the problem can begin before a customer makes their first deposit.

The consequences extend beyond fraud losses. Every additional check, intervention or disputed transaction introduces cost and complexity, while friction can discourage legitimate customers from completing transactions.

At the same time, evolving regulation is placing greater expectations on operators to verify their customers, protect vulnerable players and demonstrate that appropriate safeguards are in place. Operators must balance these obligations with the commercial realities of delivering a seamless, competitive customer experience.

Ultimately, the question is whether the industry can move beyond assessing the likelihood that a transaction is genuine, towards establishing greater certainty that it is.

Kevin Grönvall
Chief Operating Officer



The right details, the wrong person.

An online payment can contain all the correct card details, without proving that the person making it is authorised to use them.



The limits of an online payment.

At the point of payment, an online gambling operator needs to answer a deceptively simple question: *is the person making this deposit authorised to use this card?*

In an in-person card transaction, there are established ways to answer that question. The card is present, its chip can be read, and the cardholder enters their PIN. The transaction carries evidence that the physical card and its credentials were present at the point of payment.

Online, the situation is different. Card not present transactions rely on card details rather than the physical card itself. Those details may be correct, but they don't confirm that the person entering them is authorised to use the card.

The difference is reflected in industry fraud data. According to the European Banking Authority and European Central Bank, remote card payments had a fraud rate 13 times higher by transaction value than non-remote card payments in 2024, based on EU/EEA-issued cards.

The industry has developed increasingly sophisticated ways to manage this uncertainty.

Fraud detection systems analyse signals such as device, location, transaction history and behaviour. Authentication technologies, including 3D Secure, one-time passcodes and biometrics, provide additional safeguards and have made an important contribution to reducing online payment fraud.

But even with these protections, a conventional card not present transaction remains fundamentally different from one authenticated using the physical card and its chip.

This distinction has real consequences. A fraudulent deposit can quickly become an irreversible cost. Funds may be used before the legitimate cardholder discovers the transaction, leaving the operator exposed when the payment is later disputed. At the same time, additional checks designed to reduce that exposure can introduce friction for genuine players.

The challenge is to establish greater certainty at the moment the payment is made, rather than relying entirely on the controls surrounding it.



CASE STUDY

When stolen credentials are enough

A UK fraudster used stolen identity documents and multiple stolen debit cards to deposit money into an online gambling account, before attempting to withdraw the funds onto a single card. The case shows how stolen credentials can satisfy separate online checks without proving that the person behind them is the legitimate cardholder.

Signals aren't proof.

Knowing your customer is fundamental to online gambling. But establishing who opened an account, assessing whether a transaction looks suspicious, and proving that a payment is authorised are different things.

An operator may have verified a player's identity when they registered. Age checks may have established that they are legally able to gamble. Fraud systems may recognise their device and behaviour. Payment authentication may provide further confidence in a particular transaction.

Together, these controls create a picture of risk, but gaps can remain between them. A verified gambling account does not necessarily mean the person currently using it is the person who opened it. A payment card added to that account does not, by itself, establish that the account holder is authorised to use it. And a transaction that matches expected patterns can still be fraudulent.



CASE STUDY

When fraud looks normal

A regular online gambler from New Zealand disputed $7,750 in online gambling transactions made after losing her phone. Because she was already a frequent bettor, including legitimate transactions of $950 - $3,500 over short periods, the disputed payments did not appear unusual to the bank's fraud systems and therefore were not flagged.

The cost of uncertainty.

When you cannot be certain who is behind a transaction, every decision carries a trade-off. Approve a fraudulent deposit and the operator may face a chargeback after the funds have already been used. Decline a genuine transaction and the customer may simply take their business elsewhere. Introduce additional checks and you may reduce risk but also add friction to an experience where customers expect to be able to deposit and play quickly.

There are operational costs too. Fraud management requires technology, rules, monitoring and intervention. Transactions that fall outside expected patterns may need further scrutiny, while disputes and chargebacks create additional work after the transaction has taken place.

Regulation adds another dimension. Operators must not only verify who can access their platforms, but also demonstrate that safeguards around identity, age and payments are effective. The challenge is maintaining those protections without repeatedly asking legitimate players to prove themselves.



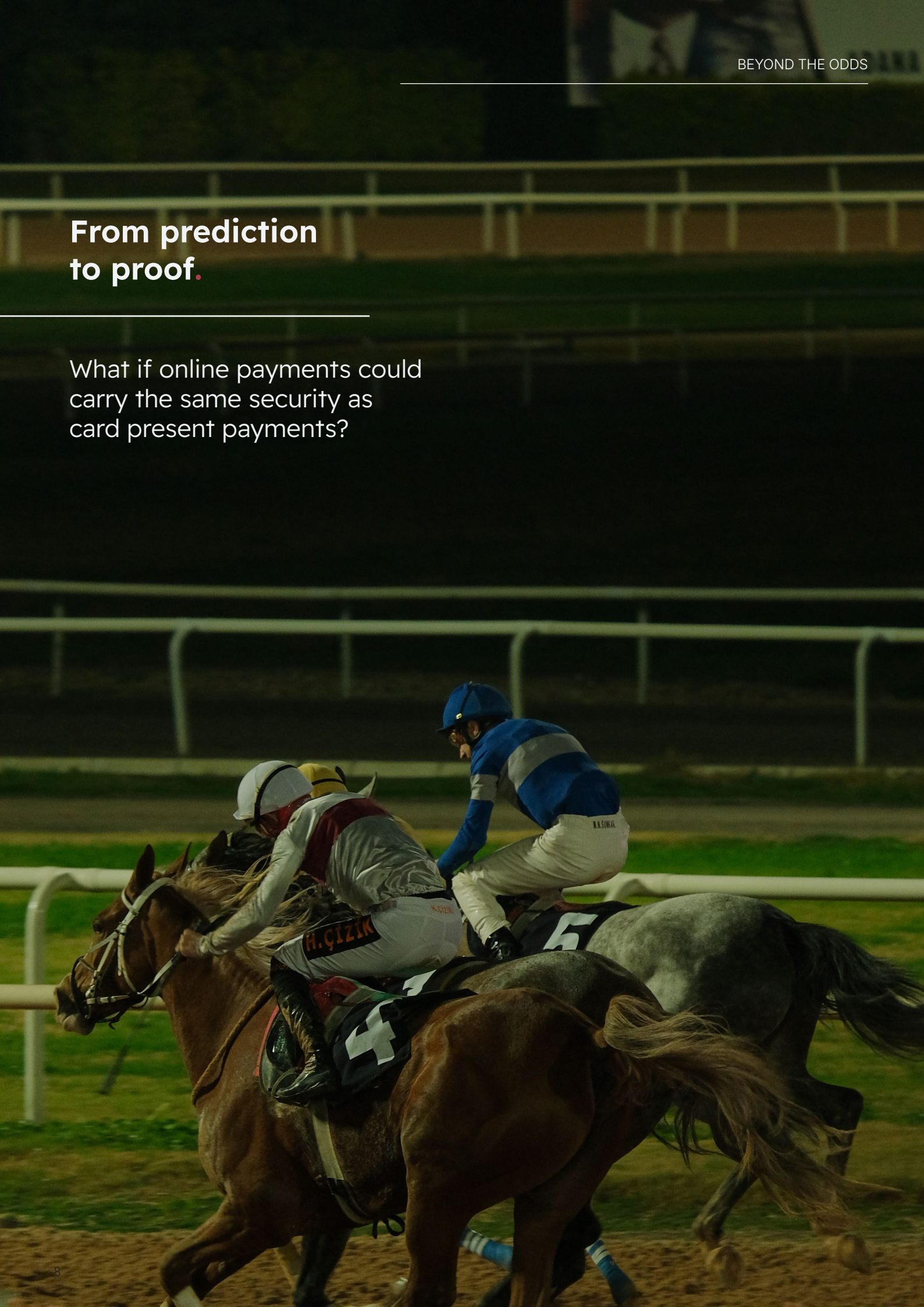
CASE STUDY

When the account is genuine, but the user isn't

A credential-stuffing attack in the US compromised around 60,000 online betting accounts. Attackers added new payment methods and used small deposits to verify them before withdrawing victims' funds. Around $600,000 was stolen from 1,600 accounts. The accounts were genuine, but the people controlling them weren't.

From prediction to proof.

What if online payments could carry the same security as card present payments?



A different approach to payment certainty.

For all the sophistication of today's fraud detection and payment authentication systems, there remains a fundamental difference between assessing the risk of a transaction and establishing direct evidence of its authorisation.

In a physical card transaction, the card's chip and PIN provide an established means of authenticating the payment. Online, the industry has largely had to compensate for the absence of that interaction through additional technologies and controls.

But what if that distinction no longer had to exist?

What if operators could bring the same card present authentication into online transactions, giving them stronger evidence of payment authorisation without relying solely on the signals surrounding it?

This isn't about throwing the baby out with the bathwater. The industry's existing controls have an important role to play. But there's an opportunity to build on them with stronger evidence that the payment itself is being legitimately authorised.



Change the transaction, change the possibilities.

One way to establish greater certainty at the point of payment is to change the nature of the transaction itself. Card Present over Internet (CPoI®) extends the familiar, globally established process of card present payments into online channels. Through a secure tap and PIN payment on their own mobile device, customers can authenticate an online gambling deposit in the same way they would at a physical payment terminal.

Importantly, this is a genuine card present transaction, rather than a card not present payment with additional authentication layered on top. The physical card and its chip participate in the transaction, with PIN verification providing stronger evidence that the person authorising the payment has both the physical card and its PIN.

For gambling operators, this opens up several possibilities:

- **Greater protection against payment fraud and chargebacks**
  Card present authentication makes stolen card details alone insufficient to complete a transaction. By operating within the card present framework, CPoI® is designed to reduce exposure to certain types of payment fraud and qualifying fraud-related chargebacks, subject to applicable scheme rules.

- **More confidence in genuine deposits**
  Transactions that might otherwise trigger additional scrutiny can be supported by stronger payment authentication, potentially reducing unnecessary declines and challenges for legitimate players.

- **A familiar payment experience**
  Tapping a card and entering a PIN is second nature to millions of consumers. Bringing that experience online offers a straightforward way to complete a deposit without manually entering card details or navigating additional authentication steps.



Old enough on paper

Verifying the account holder's age is one thing. Establishing who's behind a transaction is another.



Age assurance: another question of proof.

Verifying that players meet the legal age requirement is a fundamental regulatory obligation for online gambling operators. Identity verification services can establish a customer's age during registration, but age assurance at the point of payment offers an additional safeguard.

CPoI® supports age verification at the point of payment, allowing operators to establish whether the registered cardholder meets the required age threshold. The response is a simple yes or no, without disclosing the cardholder's date of birth or other personal information.

Combined with card present authentication online, this provides an additional layer of assurance. An age-threshold check can establish whether the registered cardholder meets the requirement, while a physical card tap and PIN provide stronger evidence that the payment instrument is present and being authenticated.

There is an important distinction, however. This does not establish the age of the individual physically holding the card, nor does it replace an operator's existing identity and age-verification obligations. It adds another source of assurance to the payment process, complementing the safeguards operators already have in place.



EXAMPLE

When a verified account isn't enough

UK government research found that 5% of 11 - 16-year-olds reported using a parent or guardian's account to gamble online with permission. The finding highlights an important gap in age assurance: verifying an adult account holder doesn't necessarily establish who is using the platform.

Building trust into every transaction.

For all the advances in online gambling, the way payments are authenticated has remained largely unchanged. And that leaves an opportunity to rethink what operators can prove, rather than simply what they can predict, at the point of payment.

The industry has made significant progress in establishing who its customers are, protecting vulnerable players and identifying suspicious activity. But there remains an important distinction between knowing who has opened an account and confirming that a particular payment is legitimately authorised.

In an industry where deposits happen in seconds and funds can be used almost immediately, that distinction matters. The consequences of getting a payment decision wrong can extend well beyond the transaction itself.

Bringing card present authentication into online gambling offers a way to close that gap, strengthening payment decisions while complementing the identity, age assurance and fraud controls already in place.

As online gambling continues to grow, building greater trust into the payment itself could give operators more confidence in every transaction, while making it simpler for legitimate customers to pay.



About Burbank.

Burbank is a payments technology company and the creator of Card Present over Internet (CPoI®), software that enables genuine card present transactions in online channels using the customer's physical card and PIN and their own mobile device.

CPoI® is designed to help merchants reduce fraud and chargebacks, approve more genuine customers and bring the security of card present payments to digital commerce.

Find out more at paywithcpoi.com

CPoI®

Burbank.