

The Fraudsters Playbook:

5 tricks that fraudsters use
to target eGaming operators



Do you want the good news or the bad news?

The good news first of course... the online gaming industry has grown by over 20% a year for the last decade¹ and including lottery purchases, nearly 75% of people are online gamblers. The US is opening up, Japan is due to turn into a huge exciting market and more European jurisdictions are licensing each year.

But don't pop the champagne cork just yet... right across the world, card fraud is on the increase again. The card fraudsters from Romania to Richmond to Reno that spend their days maxing out fraudulently obtained cards on flat screen TVs, smartphones, high-end fashion, travel and laptops need to do something to relax in the evening. And they're coming to your site...

Fraudsters love online gaming, not just in their leisure time but also in their work time. As for the supposed threat from money launderers using online gaming to cash out and launder money, well that's just a myth right? Wrong.

In this Jumio White Paper we will share the results of conversations with ex-fraudsters and law enforcement officials about how fraudsters are targeting the online gaming industry.

Here's Jumio's insight into five ways that fraudsters are targeting your eGaming operation. And how you can stop them by understanding how Jumio's computer vision is helping companies prevent fraud whilst reducing payment friction.



5 tricks that fraudsters use to target eGaming operators



1

The stacked deck

4-6

How fraudsters engineer fraud in peer-to-peer gambling



2

The lay-off

7-10

How fraudsters will try to cover their tracks on your site when using fraudulently obtained card details



3

The team wash

11-13

How fraudsters will work as a co-op to launder their proceeds of crime through peer-to-peer gambling sites



4

The gift wash

14-15

How criminals fraudulently get access to customers online wallets to wash dodgy cash into clean cash



5

For sale

16-18

The log-in details for your site that fraudsters are currently buying on the dark web



And how to stop the fraudsters coming to your site

19

1



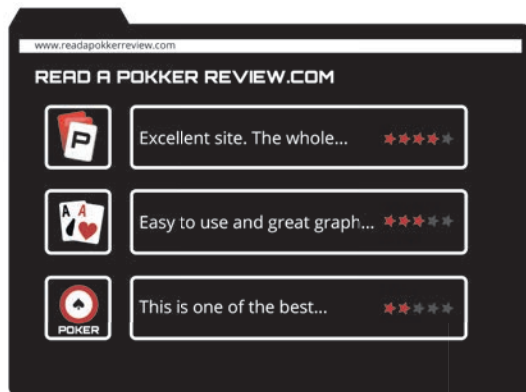
The stacked deck

How fraudsters engineer fraud in peer-to-peer gambling

When fraudsters target peer-to-peer gambling, the fraudsters aren't just trying to beat the gaming site, they're gaming the site's customers at the same time.

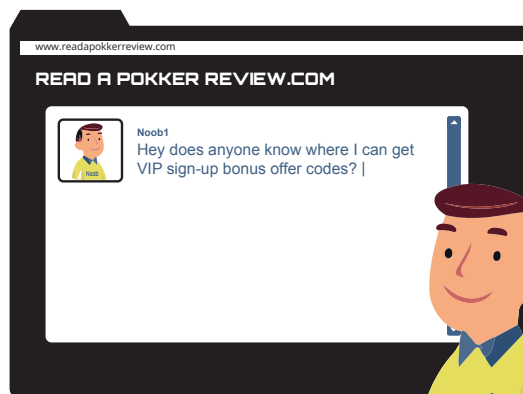
Here's a technique that we found being discussed on a fraudsters chat room called "The Stacked Deck" that fraudsters use to engineer fraud in peer-to-peer gambling such as poker.

A



Online gaming enthusiast Noob browses online gaming review sites or operators' social channels looking for the best chip bonuses.

Impressed by the social interaction, Noob asks his fellow gamblers where he can get the best odds.



B





Mr Helping Hand volunteers a great site he has just used where he got voucher codes for a load of betting sites and gets chatting with Noob, and they arrange to meet at a table once Noob has got the VIP sign-up bonuses.

Noob goes to the recommended VIP bonus site and upon clicking on the links to get latest bonus codes...surprise surprise... his device is being loaded with screen scraping malware so that the fraudster can see what Noob is doing.



Noob & Mr Helping Hand as arranged meet at a table and Mr Helping Hand kindly takes Noob to the cleaners...



“This exploit requires skills that not every fraudster has got...patience, technical know-how and the mind for the long game. Work it right and the gaming punter can be in your back-pocket for long enough to be a nice little earner.”

Ex-fraudster



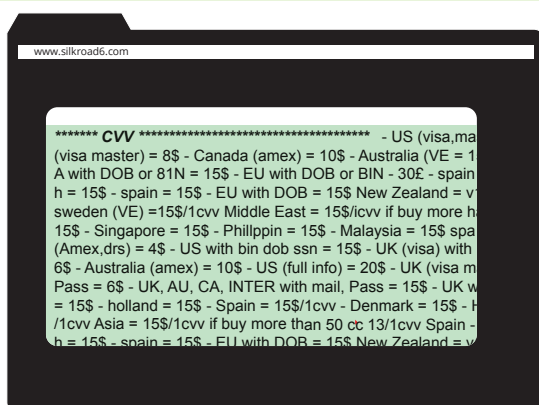
In this exploit the victim doesn't even know that they have been hit by fraud, instead putting it down to bad luck, bad cards or bad judgement. From the fraudster's perspective, one victim alone won't yield a huge return, but they can work this victim for as long as they like, tracking them across different sites and playing a long game by playing (and beating them) under different user names.



How fraudsters will try to cover their tracks on your site when using fraudulently obtained card details

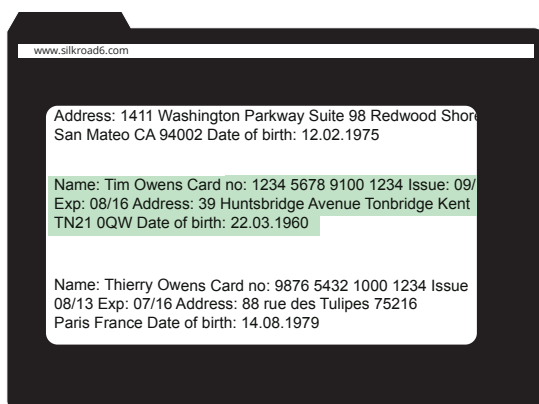
From a fraudster's perspective, their best work is done when the victim doesn't know that they have been defrauded. Here's a technique that fraudsters use with stolen cards to cover their tracks:

A



The fraudster goes shopping on fraudster chat room to prepare for the fraud.

B



The fraudster buys payment card and identity data from fraudster chat room.





www.beton81.com

BET ON 81.COM

My bets

Arsenal v Everton EVERTON TO WIN €20	LOSE €20
3.10 at Newmarket PINEAU DE RE TO WIN €15	WIN €195
Murray v Nadal NADAL TO WIN €30	LOSE €30
49ers v Raiders 49ERS TO WIN €25	LOSE €25

The fraudster uses card details to load €200 funds to a prepaid card. Money laundering regulations governing prepaid money schemes only brings Customer Identification Program or Customer Due Diligence procedures into play if the prepaid card load is greater than €999. As a result the fraudster can use whatever identity details they wish in this part of the fraud or they can use the identity data they purchased earlier.



www.beton81.com

BET ON 81.COM

Create account


Name
Tim Owens

Card Type
VISA

Card Number
1211 1019 8765 4321

Expire date
08.16

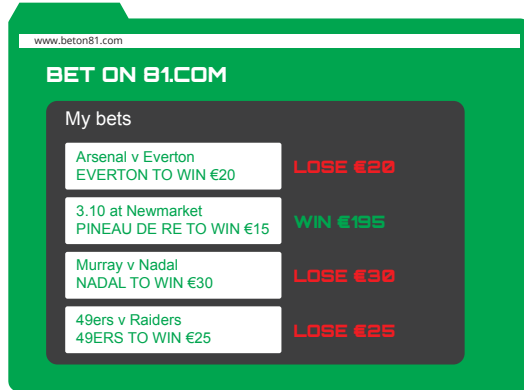
DEPOSIT
€200.00

SUBMIT 

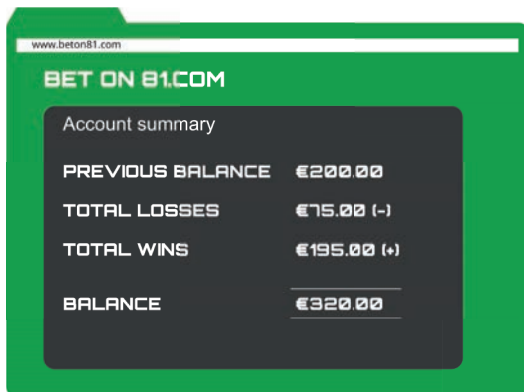
The fraudster then goes on to create an account at an online gambling site. The fraudster can proceed with fake details they are using or choose to use the real customer identity details they have obtained. Customer verification is undertaken at different levels and at different times by the gambling operator based on where they are licensed, creating loopholes for the fraudster to exploit and enabling the fraudster to learn which sites are easier to target than others.



E



The fraudster lays several bets. If they win then they are building funds that they can then withdraw to their prepaid card. If they lose then they have lost nothing but in fact have started building an account history with the operator, which they can use to their advantage at a later date.



F

But here's the clever bit... If they win, then the fraudster cashes out €200, back to the prepaid card, with which they then pay back the original €200 to the payment card used to start the fraud. The real card owner sees a €200 charge which was immediately credited back and receives an email, letter or call (from the fraudster of course) pretending to be the bank and card scheme announcing that their automated fraud detection has detected and caught the fraud attempt with no further action needed.

www.sikrads.com

Address: 1411 Washington Parkway Suite 98 Redwood Shore San Mateo CA 94002 Date of birth: 12.02.1975

Name: Tim Owens Card no: 1234 5678 9100 1234 Issue: 09/ Exp: 08/16 Address: 39 Huntsbridge Avenue Tonbridge Kent TN21 0QW Date of birth: 22.03.1960

Name: Thierry Owens Card no: 9876 5432 1000 1234 Issue: 08/13 Exp: 07/16 Address: 88 rue des Tulipes 75216 Paris France

www.prepaidcard.com

PREPAIDCARD.COM

Name: Tim Owens

Card Type: VISA

Card Number: 8180 4636 4444 7010

Expire date: 08.16

LOAD €200.00

SUBMIT

www.beton81.com

BET ON 81.COM

Create account

Name: Tim Owens

Card Type: VISA

Card Number: 8180 4636 4444 7010

Expire date: 08.16

DEPOSIT €200.00

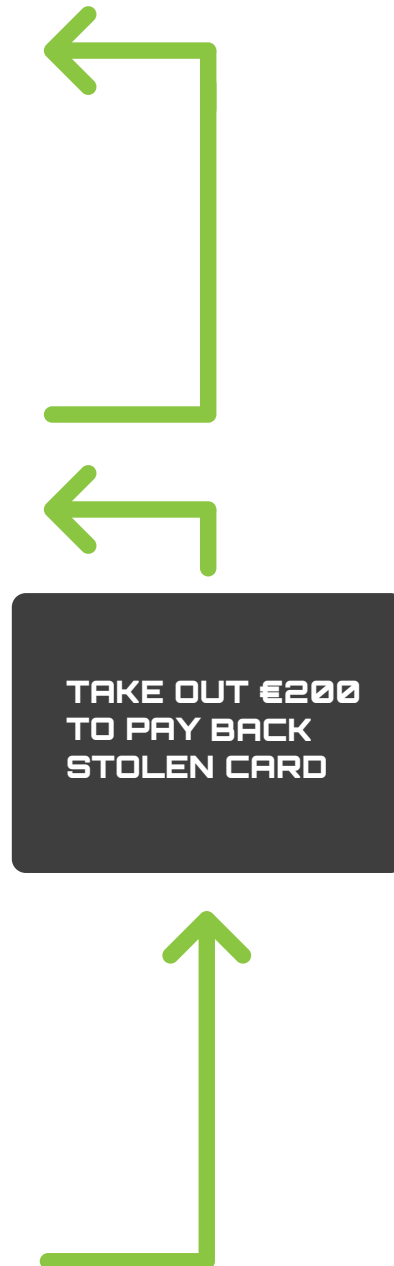
SUBMIT

www.beton81.com

BET ON 81.COM

Account summary

PREVIOUS BALANCE	€200.00
TOTAL LOSSES	€75.00 (-)
TOTAL WINS	€195.00 (+)
BALANCE	€320.00



And then the cycle begins again... fraudster loads to prepaid card, which loads to gambling account...

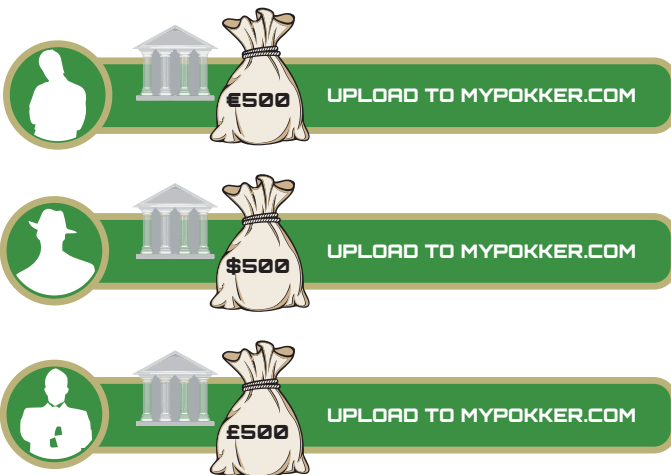


How fraudsters will work as a co-op to launder their proceeds of crime through peer-to-peer gambling sites

Gamblers want to be able to create a gaming account and cash-out in a smooth and seamless process. At the same time operators are mandated to put in place checks and balances that will detect and deter crime. Getting the balance right to keep customers coming back whilst keeping fraudsters out is a tricky balancing act.

Here is some insight as to how fraudsters told us how they work together to clean their cash on online gaming sites. “The team wash” is how fraudsters use gaming operators as conduits for money laundering.

A

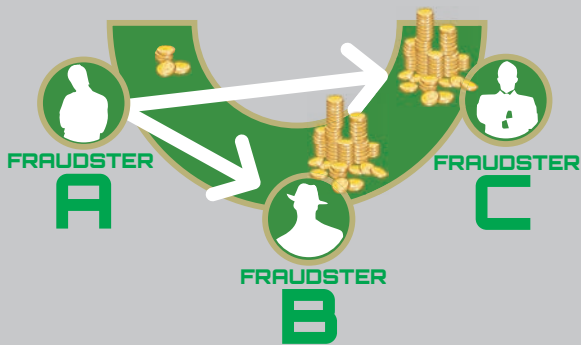


In this fraud exploit, fraudsters will club together and work as a gang to help each other launder money.

The fraudsters control bank accounts or other payment tools that are not registered in their own names. The proceeds of their crime are channeled into this account.

B

In Game 1 Fraudster A loses £435 to Fraudsters B and C.



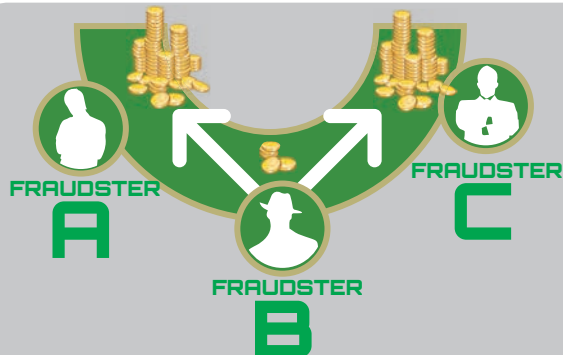
GAME 1

**FRAUDSTER A LOSES
€435 to FRAUDSTERS
B and C**

They work as a co-op together to launder their funds at online poker tables.

C

In Game 2 Fraudster B loses £410 to Fraudsters A and C.

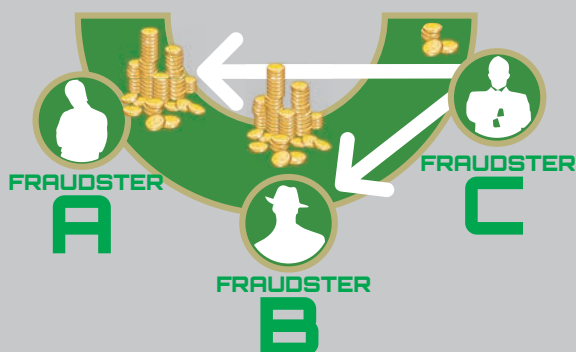


GAME 2

**FRAUDSTER B LOSES
€410 to FRAUDSTERS
A and C**

D

In Game 3 Fraudster C loses £510 to Fraudsters A and B.



GAME 3

**FRAUDSTER C LOSES
€510 to FRAUDSTERS
A and B**

“ This is not a big cash-out exploit but more of a regular little earner. Most operators are actively looking out for signs of chip dumping so the losses & wins have to stay small and under the radar. ”

Ex-fraudster



“ My team and I would have a game plan in advance and be on the mobiles or on VOIP and tell each other when to raise or fold and we would make the win/loss pattern look convincing. We would always play from our normal respective locations, at the same time of day and using the same devices, nothing that would raise the alarm at the payments team. ”

Ex-fraudster



4

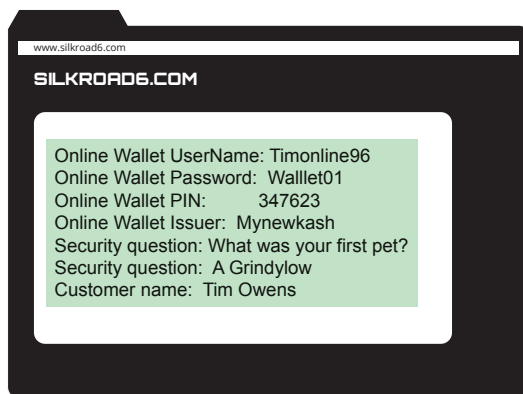


The gift wash

How fraudsters will access other people's payment tools, not to steal their money but to pass their own funds through for cleaning

This fraud exploit is one where a lone fraudster takes advantage of human nature and greed to launder money through online wallets often used by online gaming customers. Here's how it works:

A



The fraudster obtains credentials to an online wallet (the target wallet) via a fraudsters' chat room, malware attack, or Wi-Fi hack.

B



The fraudster transfers monies from their own financial instrument funded by the proceeds of crime to the target wallet.

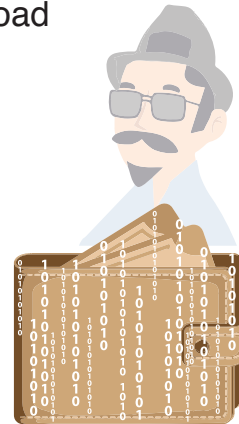
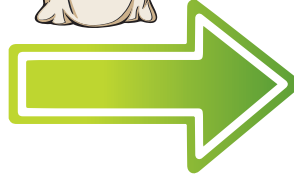


C

The fraudster uses target's wallet credentials to load €1,000 to the target wallet.



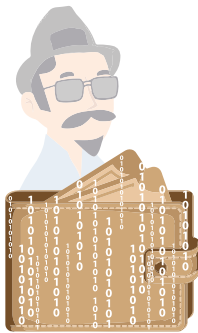
FRAUDSTER BANK



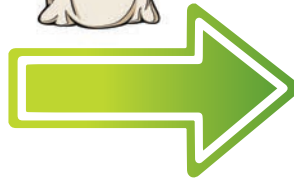
TARGET WALLET

D

The fraudster sends on €800 from target's wallet to another financial instrument they control and own in another name. In this new financial instrument the fraudster's money is clean and unassociated with the proceeds of crime.



TARGET WALLET

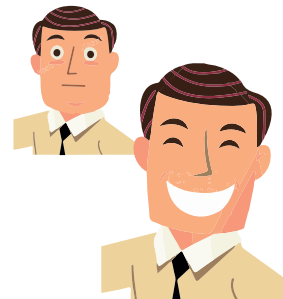
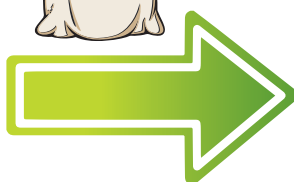


NEW FI



E

The fraudster leaves €200 in the "victims" wallet so that the victim sees it as a mistake or accounting error and has an incentive not to report the surplus €200 they find sitting in their account.



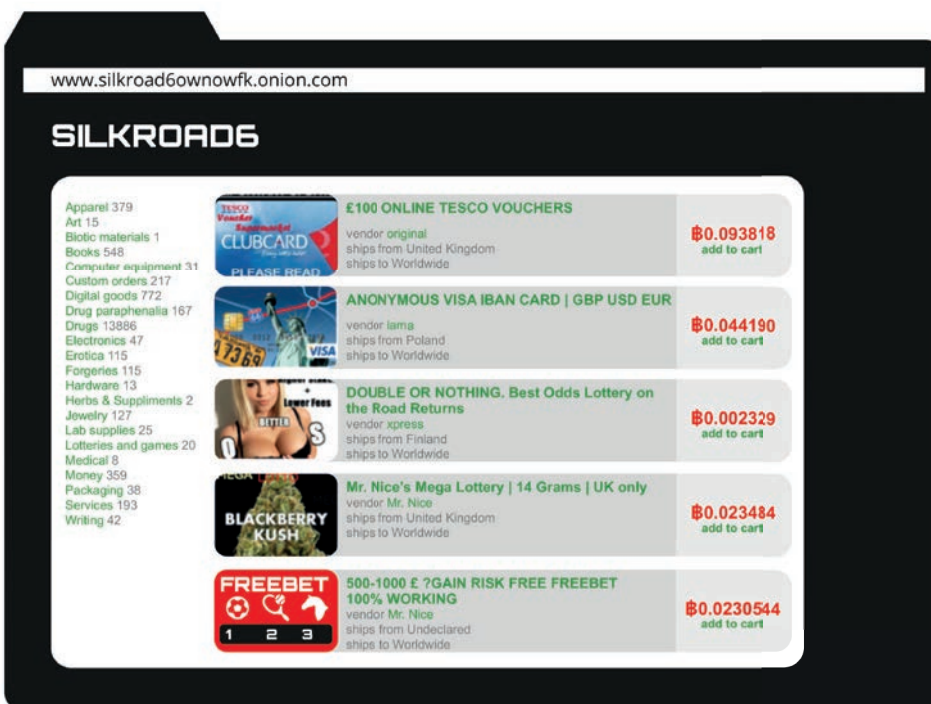
5 For sale

The tutorials, gaming site logins, and data that is currently for sale on the dark web

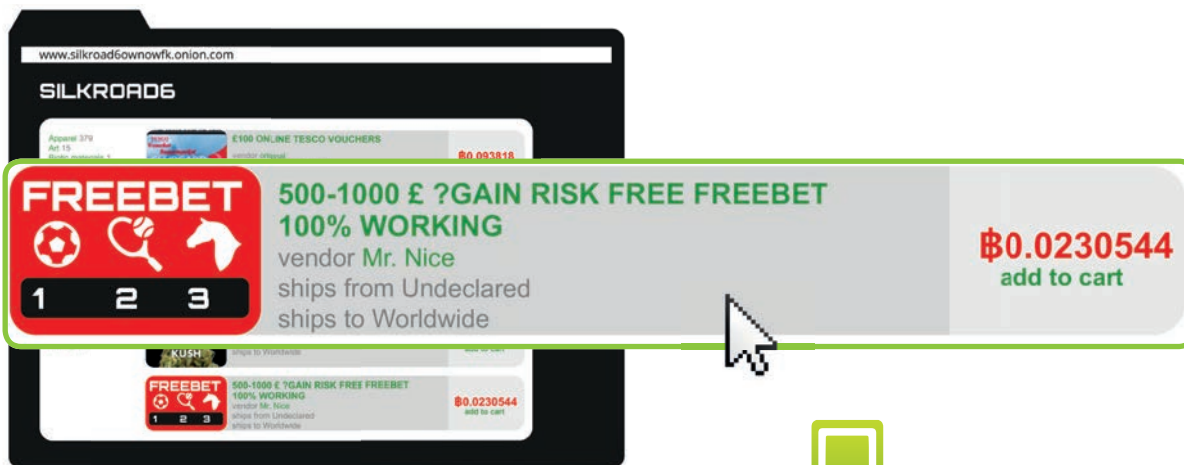
As part of our research with (ex) convicted fraudsters, we were given a brief glimpse behind the curtain, a quick tour of the dark web. Here's our insight into the sale of tutorials on how to target gaming sites, gaming site logins, and easy access to payment instruments.

Since the Silk Road was shut in 2013 by the FBI and UK's National Crime Agency, subsequent generations of it have re-spawned. In fact as of April 2014, the fraudsters are now trading on version six of the Silk Road, in itself an indication that each version of the Silk Road has a limited shelf life and is abandoned by the fraudster community before law enforcement catch-up and begin surveillance.

Of note here is the name of the site "silkroad6ownowfk.onion" showing that there are now multiple generations of silk roads. The tools available to fraudsters targeting the gaming industry include logins to bank accounts, prepaid cards and money transfer services.



Here's a sample screen shot from the Silk Road 6...



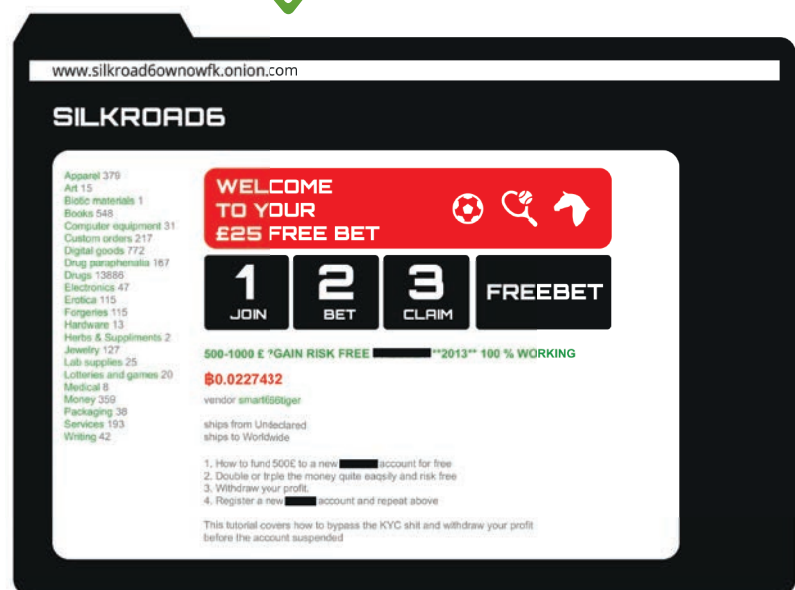
Of particular interest though is the tutorial on how to defraud one of the UK's largest betting sites.

We have edited the text and the imagery as it's not fair to expose one site alone when nearly all the large sites have been probed, analyzed and exploits produced and sold to the highest bidder.

In this tutorial, the vendor offers:

- A method for exploiting the site's free sign-up bonus
- A method as to how to "bypass the KYC stuff"

Further contact with the vendor working this particular operator reveals that the tutorial is in fact a conduit to the real product on sale, access to live accounts with live balances. The accounts are established accounts that have a transactional history. The starting rate to buy access to an account is €10, with higher funds charged for more established accounts with a higher balance.



how to "bypass the KYC stuff"

“ I didn’t specialise in one particular operator. What you find is that at times, it’s hard to open accounts with some operators but a few months later, as they tweak their policies or have a push to open new accounts they can be weaker. Word then gets out that [REDACTED] is weaker or that [REDACTED] has closed their loopholes. ”

Ex-fraudster



The laws of supply and demand are also at work here. Sometimes the fraudster will have scores of accounts opened and in which case he or she sells most of them on. When they do not have a surfeit of open accounts, they work them for their own profit.

How does Jumio tackle the fraud challenge?

Jumio

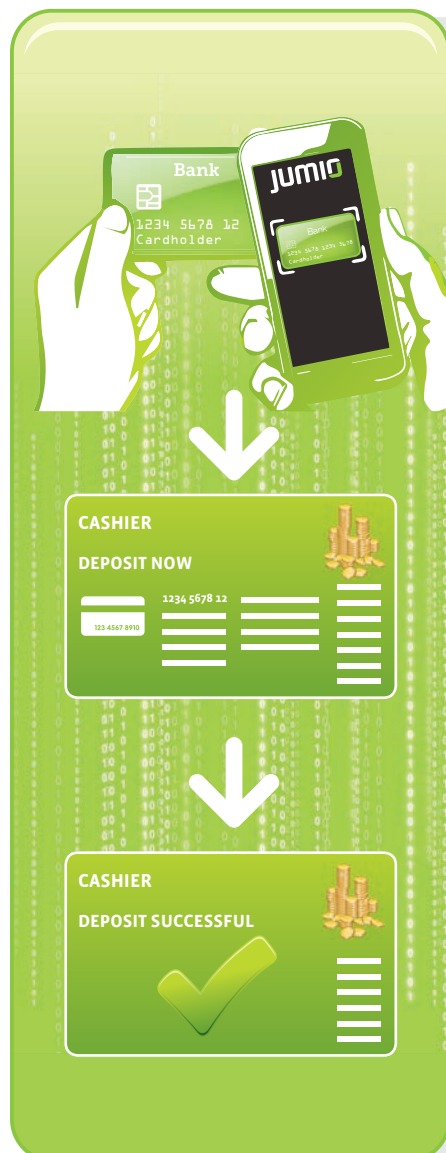
What if there was a new way of making the deposit process on gaming websites more difficult for fraudsters?

And at the same time help increase revenue by tackling the problem of transaction abandonment?

At Jumio, we specialize in computer vision, which is another way of saying that we think it's old fashioned to key in payment and personal data when we can be getting our (increasingly clever) devices to do the work for us by utilizing a webcam or a mobile device camera.

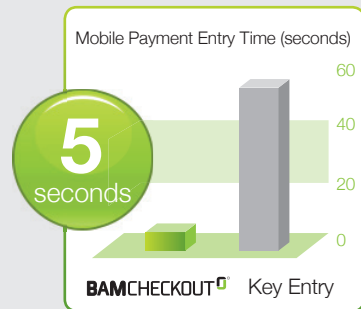
Here's a couple of examples of how Jumio's computer vision is helping companies prevent fraud whilst reducing payment friction:

How to make a card-not-present transaction more present



1

Sites using Jumio's BAM Checkout offer their customer the option to deposit by scanning their card with their device camera or webcam.



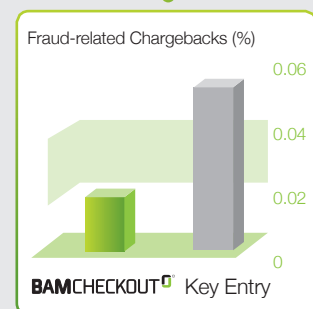
2

Jumio scans card number, expiry date, customer name (and sort code and account number if needed) and sends it directly into the payment process.



3

Customer evidences that they have the physical card and flies through deposit and transaction is complete.

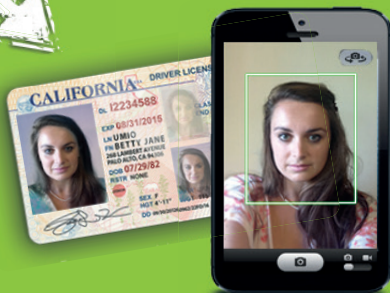


How to validate customer age and identity at account creation or pay-out as if they are standing right there in front of you

NETVERIFY[®]



Document Validation



Face Match



- ✓ Forgery check
- ✓ Hologram check
- ✓ Microprint check
- ✓ MRZ code check



- ✓ Face detection
- ✓ Image normalization
- ✓ Facial comparison
- ✓ Face match confidence rating

1

Sites using Jumio prompt customers to use the webcam or mobile device to scan their driving license, passport or other photo ID.

2

Jumio validates customer ID document and checks a range of security features.

3

Jumio captures an image of the customer via webcam or device camera and Jumio completes a Face Match to check that the face in the ID document is the same as the face behind the account creation or pay-out

Underage customers and fraudsters drop out and move onto less well protected sites.

To hear more about how fraudsters are targeting your business and how Jumio can help prevent fraud and decrease payment friction.

email: fraudplaybook@jumio.com

jumio

