jumio

WhitePaper

The Fraudsters' Playbook…

How fraudsters steal identities

Nearly two thousand years ago, the famous military strategist, Sun Tzu, wrote in his infamous book, "The Art of War" that to beat the enemy you had to get to know the enemy. It's with this in mind that Jumio is publishing this white paper to help to get to know the enemy so that we can all win more battles against the fraudsters.

> *If you know the enemy and know yourself you need not fear the results of a hundred battles.*
> Sun Tzu

The Jumio researchers spent many days talking to convicted ex-fraudsters, professional criminologists, law enforcement practitioners and fraud managers to uncover some of the exploits that fraudsters use.The content of this white paper presents what we heard first hand - how convicted fraudsters steal and exploit identities. This is the first of a series of white papers in which Jumio examines how fraudsters steal identities and then go on to conduct acts of fraud against businesses.

The first conversation with one of the convicted fraudsters we spoke to revealed a whole new dictionary of fraud terms and yielded insight into the roles of players in the underground economy.
A deeper understanding of this underground economy will help us all, as professionals in fraud prevention, and as consumers to make life harder for the fraudsters.

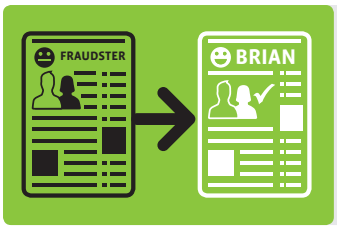
> *I can tell you all about the hackers, crackers, carders, rippers, spammers, phishers, droppers and mules.*
> Convicted Fraudster

In this, the first instalment of "The Fraudsters' Playbook" we share our insight into the first stage of the fraud process: identity theft. In our second instalment we will share our insight into the second and subsequent stages of fraud, the act of ID fraud and card fraud and how criminals profit from it. Here are our findings on five ways in which fraudsters are trying to steal your identity…

Five ways in which fraudsters steal identities…

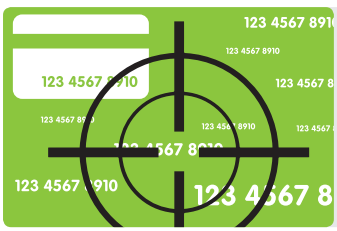
1 The Wi-Fi crack: Savour the smell of freshly roasted coffee

2 The local government census: The fraudster always knocks twice



3 Social media techniques: My virtual friend, the real life fraudster

4 The loyalty discount offer: If it looks too good to be true...



5 The Fraud Forums: Pop to the market and use the retailers' own data

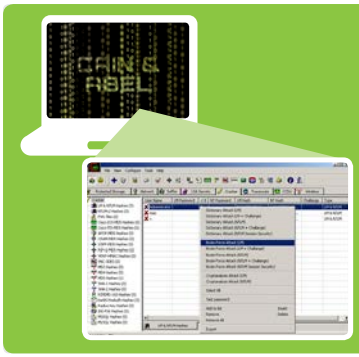
1 The Wi-Fi crack: Savour the smell of freshly roasted coffee

Next time you're stopping by your favourite coffee shop for a skinny white decaff and to catch up on emails between meetings, make sure that you use the venue's official Wi-Fi network…

One of the fraudsters' latest ploys to steal identities is to sit in a coffee shop that offers free Wi-Fi to its customers and the fraudster will use his or her laptop to broadcast a wireless network that's named exactly like the venue's official Wi-Fi. The fraudster will use that as a jumping off point to "get to know" their ID theft victim. Here's how the fraudster does it…

1 The fraudster sits in a coffee shop using his or her laptop to create a Wi-Fi hub that's identically named to the venue's legitimate Wi-Fi hotspot.

2 Coffee shop customers log onto the fraudster's hotspot, which contains malware that allows the fraudster to access their machine whilst he is sitting at a nearby table.



3 The fraudster accesses the customer's online accounts whilst sipping a latte at the same time hacking their password using fraudster cryptography tools such as Cain & Abel.

1 The Wi-Fi crack ...continued

4

Customer leaves the coffee shop and fraudster moves onto his next victim all the while amassing access to online accounts for online banking, online retail and social media ready for exploitation.

And of course, this isn't just done in coffee shops but also shopping malls, on trains, in bars, libraries, airports...

"I use a mixture of hi-tech and old school tricks to steal identities. In the summer I likes to get out for a stroll and lift bank statements from hi-density housing postboxes but the coffee shop routine gives me richer data and deeper access to my victim's financial identity."

Convicted Fraudster

2 The local government census: The fraudster always knocks twice

Next time you get a knock on your door and it's a charity collector or somebody purporting to conduct a local census, beware who you give your data to…

Here's how an organised criminal gang worked in teams to harvest large volumes of identities for fraud by pretending to be conducting a local government census and canvassing householders for identity details…

1 Fraudster selects a neighbourhood or series of streets to target and begins to build the confidence trick by putting leaflets through letterboxes the day before to advertise the census and give his gang an air of legitimacy.

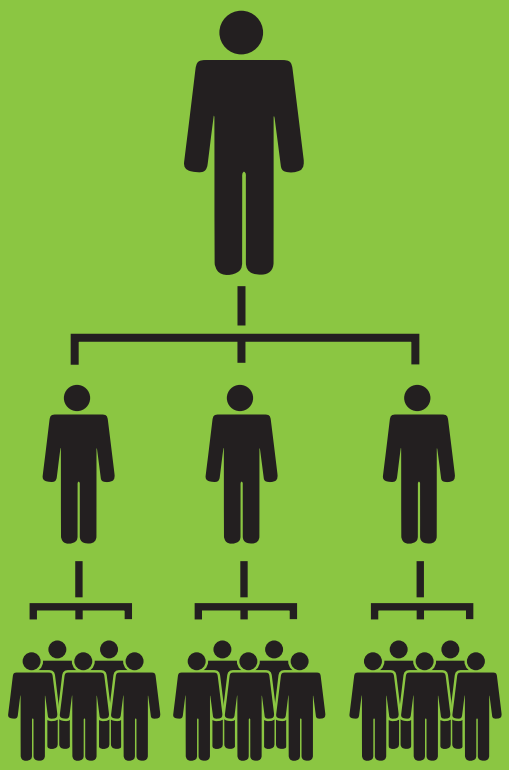
2 The fraudster's gang work in teams and canvas a street. Hand-picked to match the demographic of the neighbourhood, dressed in suits, with badges and letterheads to announce their (bogus) credentials, they figure on a one in four success rate for harvesting name, address, date of birth length of tenancy, email address and other data-points they need to commit fraud.

"Each member of my gang would hit 200 doors a day and by playing the race, gender, family or age angle as to 'how can we improve our local government service?', they would walk away with the details they wanted at least 1 in 4 times."

Convicted Fraudster

2 The local government census...continued

Here's how the operations and remuneration of such an organised gang works…



The Master

Owns, uses or sells the identities on carder forums. Has a handful of trusted fraudsters who serve as his captains in this exploit and play roles in the actual usage of the identities.

The Captains

Recruit, brief, and manage the soldiers. Captains, AKA the 10% man, get paid a percentage of their Master's frauds.

The Soldiers

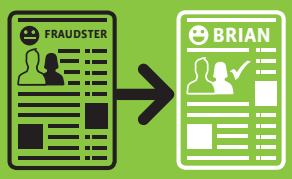
Get paid £5 or $10 for every identity they obtain.

"We would teach them which houses on a street to target and which ones not to bother with. Basically the ones with nice cars we would go for and the ones with the crappy old banger on the drive we would avoid as that was a good tell for what they had in the bank."

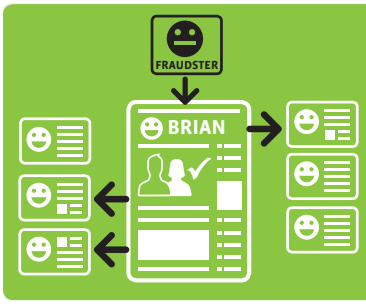
Convicted Fraudster

3 Social media techniques: My virtual friend, the real life fraudster

Much has been said in the press about how fraudsters use social media to aid the identity theft process. As a result, many social media users now don't allow people they are not connected with to see their profile and details. Here's an exclusive insight into fraudsters' social media savvy to get past privacy settings…



1 Fraudster befriends "Brian" on a social network.

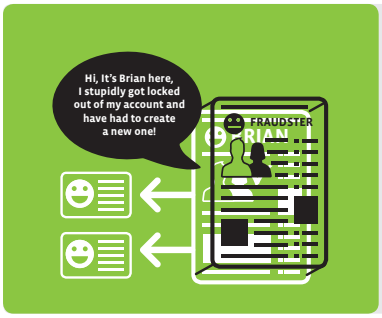


2 Fraudster checks out "Brian's" connections and friends and selects the ones that he wants to target based on how much info they display about themselves.

"This was an ID theft exploit I would use for whenever I wanted to take over somebody's identity and needed and angle, a way in. By looking at their likes I could decide which brand or retailer I could impersonate to phish them. By looking at venues and places they frequent I could decide which bar or restaurant they were at and call them to apologise that we had made a mistake and charged them too much. And of course then get their card details to process the refund…Social networks are great, whatever you want to find out about somebody to complete your ID theft…it's all there."

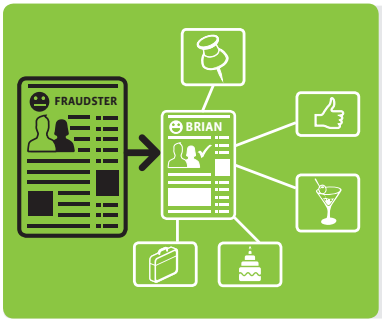
Convicted Fraudster

3 Social media techniques ...continued



3

Fraudster creates a new account for "Brian" and reaches out to the targeted connections impersonating "Brian" claiming he has lost access to his social media account and has been forced to create a new account.



4

The fraudulent "Brian" can now see all of the target connection's posts, history, likes, job titles, employers, venues, educational achievements, hobbies, where they live and really understand who they are and how they spend their time and money.

"Sometimes I would walk through their social network to find out their mother's maiden name by tracking to their mother's brother. I can't believe the lazy banks are still relying on this piece of data as a security check."

Convicted Fraudster

"My favourite targets on social media tend to be people born between 1960 and 1975. They are into social media enough to have a decent amount of data on their wall or profile but are not Internet savvy enough to protect themselves. Plus they are the perfect age to still have a good credit history and line of credit, still be economically active and also to be time-poor which makes it easier for me to con them."

Convicted Fraudster

4 The loyalty discount offer: If it looks too good to be true...

It's important to remember that fraud is just a confidence trick. Sometimes ID theft is achieved via technological means but sometimes it's just the fraudster and their wits concocting an offer that enables them to commit ID theft and walk away with the means to commit card fraud.

Here's how one fraudster uses little more than the phone book to get hold of credit card details…

1 Fraudster calls his "target" from the phone book.

2 Fraudster engages their target by masquerading as a major supermarket.

"This is my favourite technique. It's quick and easy, all I need is a phone and it has a high success rate. I walk away with all the card number details I need and I then even use their card to pay for a postal mail redirect on their card, which is the next stage of the fraud."

Convicted Fraudster

4 The loyalty discount offer ...continued

3

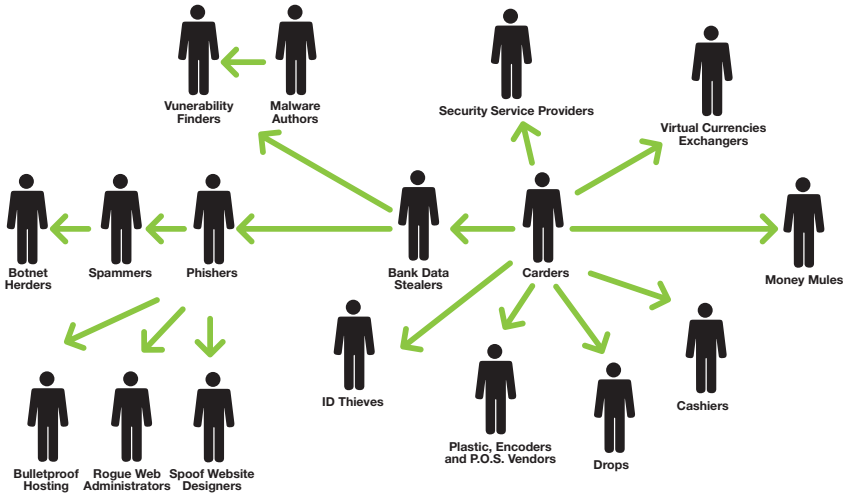
Fraudster makes their target "an offer they can't refuse". The fraudster promises unfeasibly attractive discounts off future purchases in return for a small cash payment taken via the card. The fraudster then obtains the card number and necessary details to go on to do fraud with their target's identity.

Please click here to play a recording of this convicted fraudster running this exploit and conducting the ID fraud against their unwitting target.

5 The Fraud Forums: Pop to the market and buy some data

Card fraudster communities on the web where fraudsters trade card numbers and bank account details continue to thrive, hidden in the murky reaches of the web even though the FBI and the UK's National Crime Agency occasionally shut them down.

These carding sites drive the underground economy in card fraud and there is a complex ecosystem of contractors who provide their specialist skills to help fraudsters obtain stolen identities.

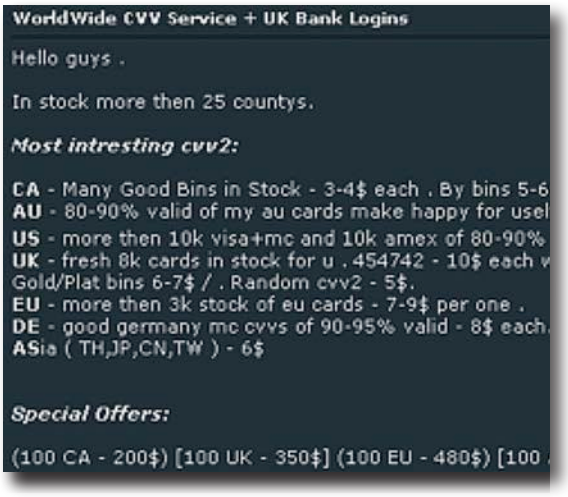


The Underground Economy[1]

A recent paper by leading criminologists Webber, Shadbolt and Yip[1] highlights the range of contractors and skills that come together to drive identity theft and the resulting identity fraud and card fraud that fraudsters implement.

Fraudsters are currently being more discerning about what data they are buying from the ID thieves. This is in part due to a high fail rate when fraudsters buy card details that don't work. A scan of customer reviews on carder sites suggests that a success rate of 60% on purchase card data is a good yield. "Grade 1" cards are unused and dependent on credit limit are generally sold for £100 or $200 each, whilst "Grade 2" cards are second-hand and sell for £50 or $100 each on the premise that they are more likely to have been cancelled and therefore fewer will work.

As such, fraudsters are now more targeted in the data that they purchase and the cards that they are interested in. In particular fraudsters will look to buy cards that begin with a specific 6 numbers (known as the Issuer or Bank Identification Number) that belong to cards issued some time ago. The tactic here is that older cards belong to older cardholders who have a better line of credit than younger cardholders.


WorldWide CVV Service + UK Bank Logins

Hello guys .

In stock more then 25 countys.

Most intresting cvv2:

CA - Many Good Bins in Stock - 3-4$ each . By bins 5-6
AU - 80-90% valid of my au cards make happy for usel
US - more then 10k visa+mc and 10k amex of 80-90%
UK - fresh 8k cards in stock for u . 454742 - 10$ each v
Gold/Plat bins 6-7$ / . Random cvv2 - 5$.
EU - more then 3k stock of eu cards - 7-9$ per one .
DE - good germany mc cvvs of 90-95% valid - 8$ each.
ASia (TH,JP,CN,TW) - 6$

Special Offers:

(100 CA - 200$) [100 UK - 350$] (100 EU - 480$) [100

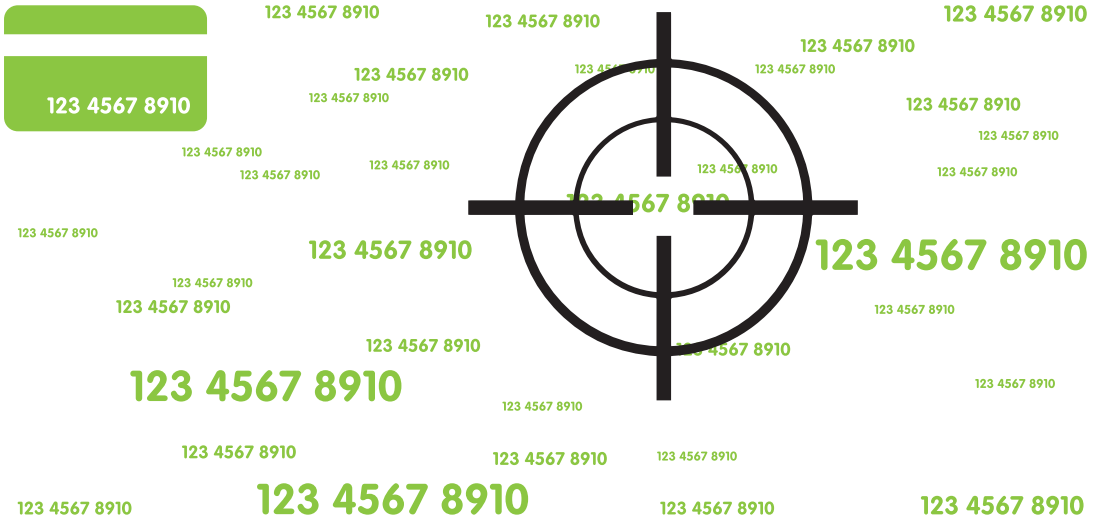
Typical post in a carding forum

1 Why Forums? An Empirical Analysis into the Facilitating Factors of Card Forums. Michael Yip, Nigel Shadbolt and Craig Webber

5 The fraud forums ...continued

“Stock” in online carder shops is commonly replenished by way of data breaches from online retailers and payment processors.

Sometimes of course tokenisation by the retailer or the processor means the ID thieves come away with only partial card digits. That however doesn’t stop the fraudsters who are ready to buy more than just the card numbers. The customer email address, username, password and billing and delivery address are of immense value to fraudsters.



How does Jumio tackle the fraud challenge?

What if there was a new way of implementing checkout on websites to make life difficult for fraudsters and at the same time help increase revenue by tackling the problem of basket abandonment?

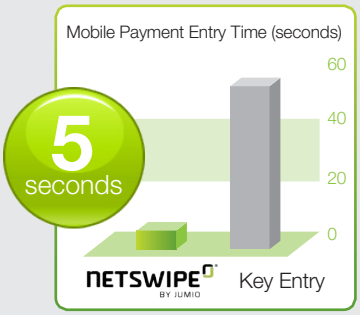
At Jumio, we specialise in computer vision which is another way of saying that we think it's old fashioned to key in payment and personal data when we can be getting our (increasingly clever) devices to do the work for us by utilizing a webcam or a mobile device camera.

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 offer their customer the option to checkout by scanning their card with their device camera or webcam.

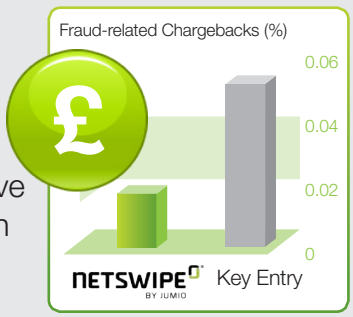


2

Jumio scans card number, expiry date, customer name (and sort code and account number if needed) and sends directly into checkout basket.

3

Customer evidences that they have the physical card and flies through checkout and order is complete.



How to validate high-risk transactions as if the customer is standing right there in front of you

Sites using Jumio offer their customer the option to checkout by scanning their card with their device camera or webcam.

1

Sites using Jumio prompt high-risk customers/transactions to use the webcam or mobile device to scan their driving licence or other photo ID

…fraudsters drop out and move onto less well protected sites.

2

Jumio validates customer ID document and checks the security features.

3

Jumio captures 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 transaction

…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 your fraud and decrease payment friction

email: fraudplaybook@jumio.com