

192 Fraud-ID

Shared fraud alert data from major retailers



What do we know about the fraudster?

As providers of CNP fraud prevention solutions we've invested some time getting to know the fraudster to better help merchants to defend their operation from fraud. Through interviews with fraudsters and by visiting fraudster chat rooms we know that fraudsters share information about which sites are "cardable" and present an easy target. In fact, fraudsters even sell identities complete with credit card and bank account data through their chat rooms.

Surely it's about time that we take a stand and share our own information in the fight against the fraudster?



And what do you know about the fraudster?

Would it be a fair assumption to make that fraudsters visit your site? Do you keep records of the fraud that you suffer and the fraud that you do catch before you approve a transaction?

What if we could all share this knowledge about the fraudsters? What if you knew the credit card numbers, the delivery addresses, the names, the email addresses and the IP addresses from the fraud that your industry peers are experiencing?

So what do we know together?

If we act collectively surely we would all know enough about the fraudsters to be able to block a large portion of their fraud attempts?

If several large retailers were to tell us all about a certain Mr Ivor Stollenkard trying to use a stolen card to get goods delivered to an address in South East London, would it make sense for you to flag that card, name and address if it gets presented as a transaction to your site?

Well now we have this information and it's time to fight the problem of CNP fraud together by pooling our collective picture of the fraudster.

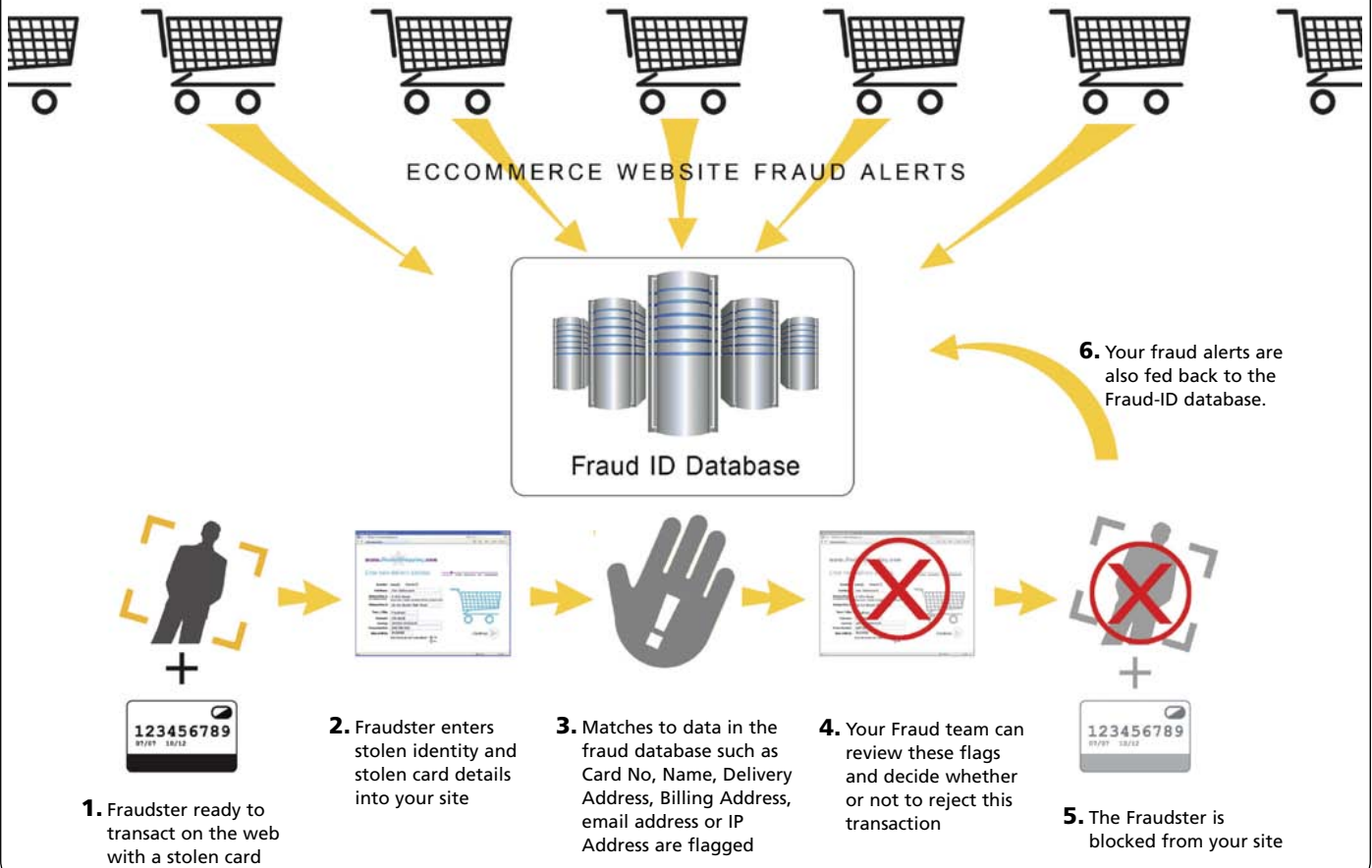
Here's how it works.

1. You give us the details of the transactions that you've identified as fraud and decided not to pass or approve
2. We allow other ecommerce brands to check these fraud alert details so they don't get beaten by the same fraudster
3. You get to check your transaction flow against the fraud alert details that other ecommerce brands have identified as fraud

And the result? - Fraudsters are locked out.

How does shared fraud alert data make the difference?

Here's a depiction of how a pooled industry fraud alert database will work for your ecommerce brand



As an industry, how do we make it work?

We've seen industry schemes like this before and to make this one work we're setting up some rules of engagement that members must adhere to:

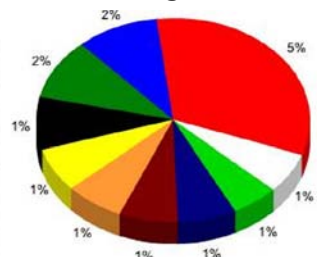
- You can only use the fraud alerts if you contribute all your company's fraud alert data on a regular basis to the Fraud-ID database
- Fraud alert data is defined as suspected or confirmed fraud
- The data contributor must have manually reviewed the transaction and decided that it was fraud
- Fraud-ID is not a blacklist
- Adhere to all of the above to ensure that Fraud-ID complies to the Data Protection Act

Fraud intelligence for UK Plc

Having identified where your fraud and your industry colleagues fraud is coming from, 192 Fraud-ID also generates reports and statistics for your review. What's the point in having this data unless we use it for intelligence too?

- Why not use the fraud hotspot data to give your call centre and your deliveries team a heads-up?
- Make more informed decisions on customers in the referral queue by searching Fraud-ID for patterns and instances around suspicious transactions
- Use the data in 192 Fraud-ID for your fraud investigations

Postcode	Count
SW1V2RD	23
SE280LY	7
SE280NE	7
SE186PL	6
SE185SG	5
B19 1LT	5
E3 2NX	5
E3 2PD	5
DA8 2NY	4
E5 5PY	4



To find out more

Call our payments ID verification team on 00 44 (0)207 909 2192

Request a call back at www.192business.com/contact

Email us your questions at id@192.com

See more on our verification technologies at www.192business.com