Are you treating your customers like criminals?

How etailers can increase sales conversions & create frictionless customer experiences...

...whilst cutting online losses and the cost of managing fraud

A report by ThreatMetrix®
BUILDING TRUST ON THE INTERNET™

A report by ThreatMetrix, validated by the ThreatMetrix Cybercrime Index.

How would you feel if your favourite retailer called the Police to arrest you as you came in the door?

or

If your favourite restaurant sent you off to the cashpoint in the rain to get cash because all your credit cards had been rejected?

or

You were taken out of the supermarket checkout queue to answer a few questions to prove your identity before being allowed to purchase

or

The border you had passed through every day for years was suddenly shut in your face?

or

You bought a gift abroad and your home bank declined the transaction on all your cards?

What's wrong with current fraud detection systems?

Every day, in store and online, retailers turn business from loyal customers away because their fraud systems lack the intelligence to identify that they are genuine, and because customers are turned off by burdensome second level authentication such as 3DSecure, and abandon their basket.

The traditional approach shifts the burden of additional authentication to customers – making the process complex, time-consuming and effortful. As a result, retailers risk potential customer abandonment and damage to their brand.

And if retailers fail to recognise customers, the authentication process involves changing forgotten passwords or other verification details, which makes users even more likely to give up.

In fact, the way retailers currently manage fraud reduction is costing them millions in lost income and lost customers.

How to tackle fraud and lose money

Spend huge sums in attracting, retaining and cross selling to customers only to not recognise them when they come to buy

Implement fraud systems that are so strict they prevent you from going into new markets

Set up a huge department of people to manually prevent genuine customers from getting caught in fraud filters

Reject a customer, let them through and then reject them again

Lower your fraud barriers at peak trading periods - such as Easter, Back to School, Christmas and New Year sales, in order to avoid the risk of blocking genuine customers, and so let in criminals, with the result that you end up paying chargeback fines and possibly higher interchange fees

Did I marry a monster?

Retailers current fraud systems often confuse fraudulent with genuine customers.

Genuine customers who look like criminals:

- Privacy conscious tech boomers that regularly clear cookies
- Employees, WiFi hotspot users and lodgers at hotels that share IP addresses or devices that are blacklisted or have negative reputation because they have been infected or compromised by malware
- Business travellers that have irregular locations and times of day

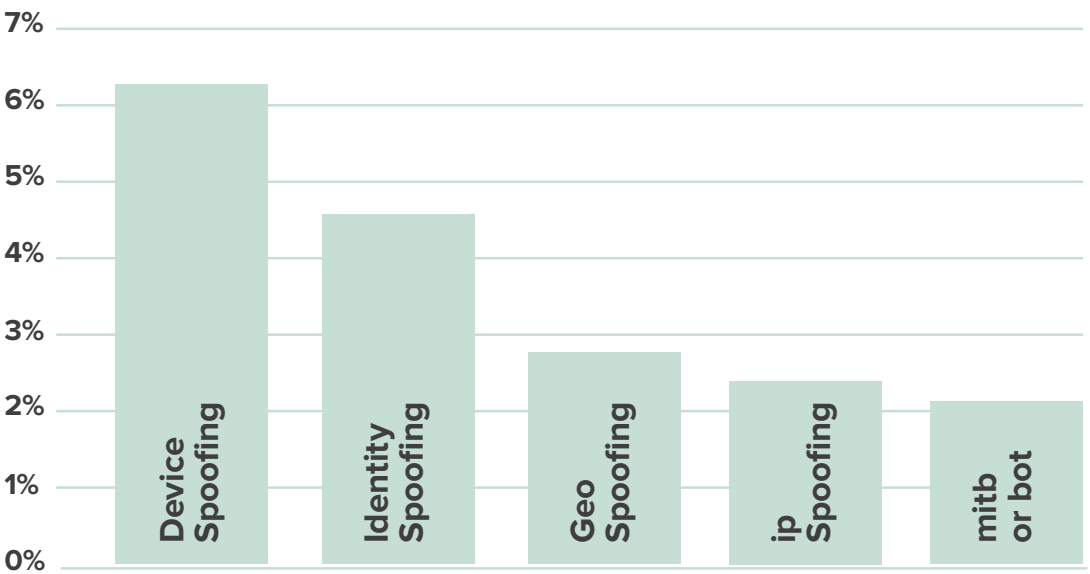
Criminals who look like customers:

- Phishers
- Man-in-the-middle
- Malwarers
- Criminals who try to create genuine personas on social media and dating sites

Did I marry a monster?

Retailers' current fraud systems often confuse fraudulent with genuine customers.

% High Risk Attack Methods



Source: ThreatMetrix Q4 CyberCrime Index

Adding to this problem, the way consumers buy from and communicate with merchants has changed. Shoppers are increasingly shifting from fixed to mobile devices – **25% of transactions are now made via mobile**[1] – which are harder to trace and secure.

Where shoppers identify themselves via mobile devices, retailers often reject a genuine customer because they are using a new smartphone, while they accept a fraudulent transaction from a phone that has been stolen.

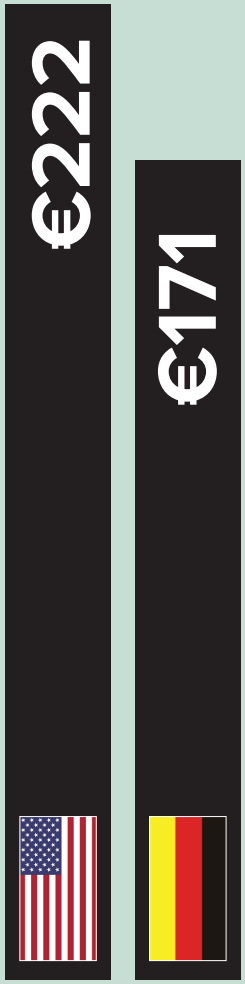
1. ThreatMetrix Q4 CyberCrime Index

What is the cost of fraud to retailers?

Fraud prevention is important but it is expensive, and new and emerging threats are not only increasing its costs, but also showing up the weaknesses in current techniques. As a result, major data breaches are happening almost every day.

According to Ponemon's 2013 Cost of Data Breach Study, each compromised record costs €222 in the U.S. and €171 in Germany. For retailers, banks, or social networks with hundreds of thousands or even millions of stored identities, this figure represents a significant liability.

While it is critical to counter these threats, it is also time to think again about whether this the right approach. After all, fraud takes the lion's share of the money spent on authentication. Fraud prevention should be spending more time helping the sales team to sell more.



98% of fraud prevention is down to better customer authentication

It is time for senior executives to find a new approach

A new approach is needed

The problem is, to most fraud prevention systems, genuine and fraudulent personas can look the same, and anomalies are often either not spotted or spotted too late.

The fraud prevention budget is being wasted on doing manual checks to stop legitimate customers falling into fraud filters that are simply too blunt and create many false positives.

Merchants need to:

Simplify customer authentication

Make it easier for consumers to buy, by making the process of identify themselves easier.

Mitigate the business impact of fraudulent activity

Fraud has an enormous cost consequence for companies – non-compliance fines, issuer penalties, low basket conversions, chargebacks, issuer penalties and so on. It is also a drain on time and resources.

Better identify real customers

Treat people like people – If you know who customers are based on real personas, then you have a more accurate measure of the risk of doing business with them. Determine key information like who and where they are, what device they are using and what they were doing last time they connected.

How to do it better

Billions of users accounts have been compromised in recent years and this creates a major risk to your enterprise. To reduce the chance of falling victim, retailers need to adopt a single platform that provides comprehensive context-based authentication and persona recognition.

This approach provides real-time defence to minimise credit card fraud and account takeover risks, while keeping the customer experience hassle-free and protecting their account login.

How to do it better

Here are some further ways in which a single, integrated system protects enterprise accounts:

Use multi-factor authentication to positively identify who is attempting access

Discover suspicious patterns of login requests or unauthorized password sharing

Detect access attempts from unknown, risky or compromised devices

Detect access attempts from user credentials that are known to have been compromised

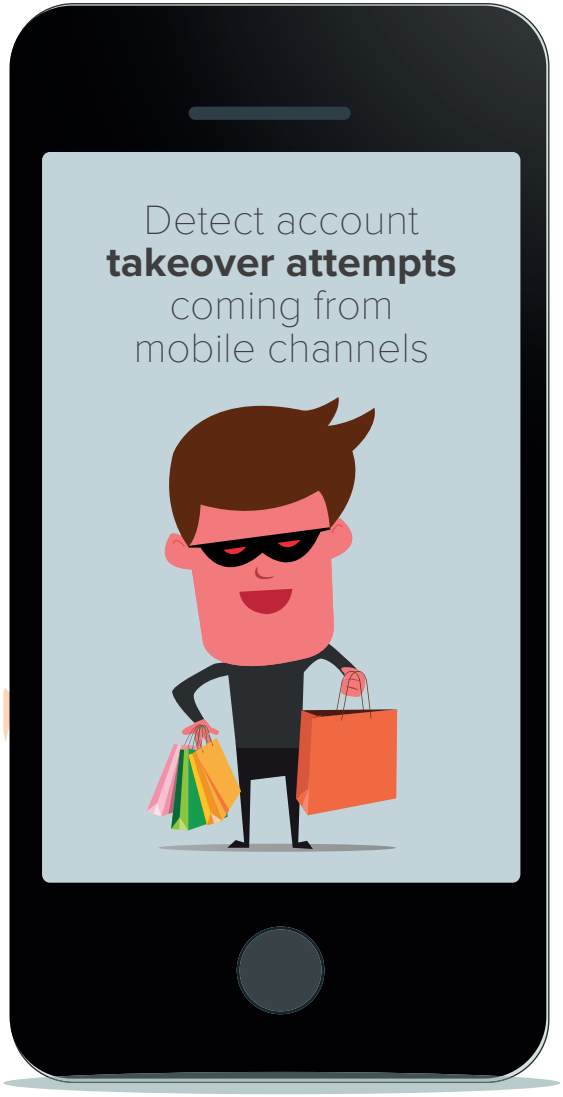
Discover malware that has infiltrated a legitimate user's device

Detect suspicious computer configurations, including oddly configured mobile devices or devices disguising their geo-location

Find logins coming from the wrong places, including devices connecting from known botnets or from behind hidden proxies or VPNs

Detect and prevent activity from bots, botnets and other scripted mechanisms

Detect account takeover attempts coming from mobile channels



The benefits of this approach

There are some things money can't buy; reputation is one of them. Enhancing fraud prevention in a consumer-friendly manner makes it easier to do business. Therefore shoppers will buy from you more often and are more likely to recommend your services.

From a user experience perspective, a single platform shifts the focus from exclusion to inclusion and balances the protection of digital assets with customer requirements.

And of course, it enables you to make more money – both through cutting fraud detection costs and the increased business it generates.

The benefits in numbers

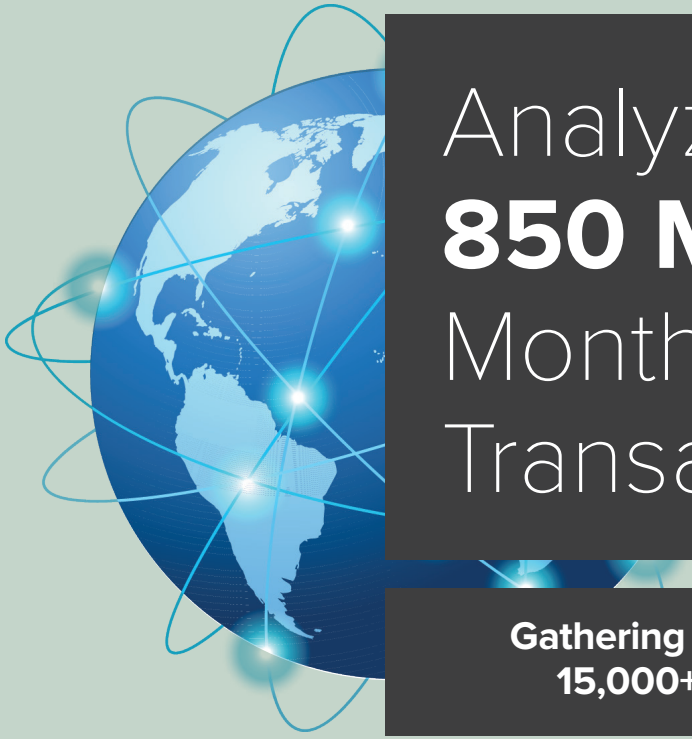
50% Reduction in Review Rates

70% Reduction in False Positives

50% Reduction in Cart Abandonment

50% Reduction in Fraud Loss

The benefits in figures

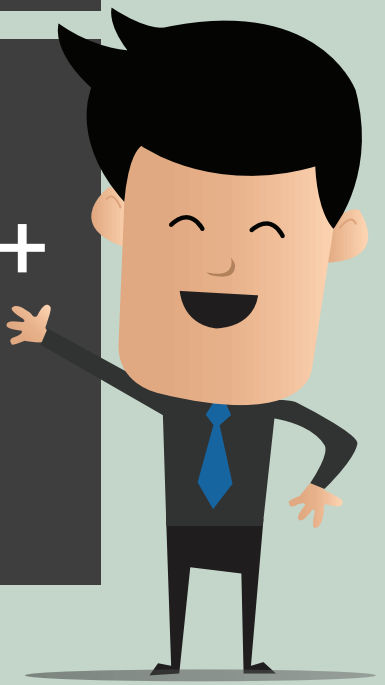


Analyzing
850 Million+
Monthly
Transactions

Gathering Insight From 15,000+ Websites

Protecting 3,000+ Customers

Defending
210 million+
Active User
Accounts



Source: ThreatMetrix Global Trust Intelligence Network

Start your fraud prevention journey

ThreatMetrix™ provides sophisticated context aware authentication solutions that leverage the collective power of a Global Trust Intelligence Network to deliver unmatched security and fraud prevention.

Contact ThreatMetrix today and discover how you can increase revenues and mitigate risks, by distinguishing between the returning customers or employees you value and the malicious cybercriminals you need to exclude.

+44 (0)1483 330013

Sales@threatmetrix.com

www.threatmetrix.com

About the report

Cybercrime Index data was generated using ThreatMetrix Global Trust Intelligence Network, which provides automated and anonymized customer, threat and fraud intelligence using real-time device, identity, behavior and reputation analytics.

The Cybercrime Index is based on actual cybercrime attacks as detected and scored by The Network's customers during the real-time evaluation of an online payment, login or new account registration.

A report by

ThreatMetrix™