ALPHACOMM

HOW YOU CAN ELIMINATE ONLINE PAYMENT FRAUD

Remote channel merchants are more vulnerable than ever to payment fraud. Thankfully, it's possible to beat fraudsters at their own game.

DISCOVER HOW »

If you sell goods or services online, especially high-risk categories like digital goods, gambling, airline tickets and electronics, you're a prime target to fraudsters around the globe.

You might as well have a sign on your website saying, 'Money Here for the Taking'.

But if you think the majority of online misconduct originates in countries like Nigeria and Bangladesh, think again. Europe is the world's key cybercrime hub, according to recent **cybercrime report by ThreatMetrix**.

True, there's an increasing number of fraud attacks coming from emerging and growing economies (attacks are defined as the number of successful and unsuccessful fraud attempts).

But the **top five countries originating cybercrime** are the US, the UK, France, Germany and Italy. Pretty advanced economies, last time I checked.

And the US is not actually biggest culprit.

Apparently, Europe originates 50% more fraud attacks than North America does, even though the US processes more online transactions than any other region.

Add to that the fact that Europe processes more mobile transactions than the US (51% and 43% of total online transaction respectively), and you start to get an idea **just how vulnerable European online merchants are**.

Before I move on to the best ways to mitigate and eliminate payment fraud, I'd like to sketch for you the current payment fraud landscape.

Online fraud attacks are now overtaking online transaction volume by 50%, demonstrating the increased level of risk for digital merchants.

Source: ThreatMetrix 'Cybercrime Report Q1 2017'

CYBERCRIME AND THREAT ATTACKS BECOME MORE ELABORATE

The techniques employed by cybercriminals grow ever more sophisticated, and companies of all shapes and sizes face a mountain of threat levels.

How likely your company is to be targeted by fraudsters depends on many factors. Those include the sales channel and industry you work in, the fraud awareness maturity of your market, the security of your IT infrastructure, as well as consumer behaviour and regional regulatory environment.

Larger merchants that sell through multiple channels experience the highest level of successful fraud attempts, with mobile channels being especially hard hit.

Do you recall all those data breaches reported on the news in the last couple of years? Yahoo!, Gmail, eBay, US voter database, Anthem to name but a few.

They're just the tip of the iceberg.

The staggering rise in data breaches has led to an increase in fraud attacks across the globe. Not surprising when you consider that 59% of data breaches in 2016 are related to identity theft.

Payment transactions are still seen by fraudsters as the most lucrative target, so say respondents to ThreatMetrix' survey. However, account login transactions are increasingly being targeted by fraudsters trying to infiltrate trusted user accounts (150% year-on-year increase).

Once they're in, they have access to all the data they need to carry out a broad range of fraudulent transactions.

Fast-evolving attack techniques employed by cybercriminals

Device spoofing
masquerading as a legitimate customer to evade device recognition and detection capabilities

Location manipulation
masking the fraudster's true location by manipulating their location tracking

Malware botnets
looking for vulnerable devices across the internet so it can infect as many connected devices as possible

Identity fraud
harvesting identity data via data breaches and the dark web to create near-perfect matches of real identities

Source: ThreatMetrix 'Cybercrime Report Q1 2017'

CROSS-BORDER AND DIGITAL-GOODS TRANSACTIONS MOST AT RISK

The growth of international e-commerce is also fuelling fraud attacks. ThreatMetrix tells us that approximately 25% of all online transactions are cross border, and cross-border transactions are 1.7 times more likely to be subject to identity fraud and 6.6 times more likely to be rejected compared to domestic transactions.

Businesses often reject transactions that originate from specific countries. Blacklisting certain regions is a way of reducing your fraud risk. Of course, the more transactions you reject, the higher the risk is of rejecting transactions from good customers. It's a common business dilemma.

In 2016, PYMNTS.com issued its global fraud attack index. This measures the growth or decline of fraud attacks on US merchant websites. Some of the statistics are startling, especially for merchants of digital goods.

The attack rate for digital goods between Q1 and Q4 2015 more than quadrupled, and almost $8 out of $100 spent on digital goods is at risk. The only category that beats it is luxury goods, which loses almost $9 out of every $100 it generates.

The airline industry is the industry most targeted by fraudsters, according to an RSA survey on e-commerce merchants and fraud in October 2014. Coming in second and third place are money transfer service providers and computer electronic sellers. Other industries greatly affected by fraud include prepaid top-ups, travel, gambling and gaming.

The Financial Impact of Fraud on Merchants

Fraud costs merchants more than 7.5% of their annual revenue.
False positives account for 2.8% of revenue lost.
Fraud and chargeback management consume between 14% and 23% of operational budgets.
Digital goods merchants suffered the worst losses, at 8.6% of revenue on average.

Source: Javelin Strategy, 'The Financial Impact of Fraud: Merchants Challenged as E-Commerce Fraud Rises Post-EMV', Oct 2016

NOW THAT YOU'RE PROBABLY CONSIDERING WINDING UP YOUR ONLINE BUSINESS AFTER READING ALL THESE SCARY STATISTICS, I'D LIKE TO SHOW YOU THAT IT IS POSSIBLE TO BEAT FRAUDSTERS AT THEIR OWN GAME.

Admittedly, it's not easy. It takes knowledge, effort, persistence and a realistic budget.

But it can be done.

Read on to discover how you can protect your revenue.

HOW TO COMBAT ONLINE FRAUD: USING THE RIGHT TOOLS FOR THE JOB

To combat fraud, it's best to tackle it from four different angles:

1 **Fraud protection**

2 **Fraud detection**

3 **Fraud prevention**

4 **Fraud elimination**

1. ONLINE FRAUD PROTECTION

To protect yourself from online fraud, you need to be aware of all the different types of payment fraud that your business is susceptible to. Believe me, it's a lot.

Then you need to know which tools and processes are available to help you detect, prevent and eliminate all those different types of fraud. There are many ways you can protect yourself against cybercrime, including:

- educating your staff about fraud and training them to be ever-vigilant
- implementing and strictly enforcing a password policy
- maintaining a secure IT infrastructure and keeping security patches up-to-date
- complying with Payment Card Industry Security Standards Council (PCI)
- using an advanced payment gateway that offers all the latest security measures, integrates with all your sales channels, and offers 100% payment guarantee

Obviously, as an online merchant, you're not expected to know all this. After all, it's not your core business. But there are fraud prevention experts out there who know just what your particular risks are.

2. ONLINE FRAUD DETECTION

This is all about spotting fraudsters trying to make a purchase via your website or mobile app using stolen data and information. In other words, it is not about stopping the fraud itself, but about monitoring fraud attempts.

The most advanced way of doing this is with advanced fraud behavioural analytics. This is self-learning software that can adapt to the ever-changing fraud environment. It doesn't limit itself to analysing transactions. It also analyses, in or near to real-time, everything a visitor to your website or mobile app looks at or clicks on.

If risky behaviour is suspected, the software automatically adds one or more layers of authentication controls. This not only gives you enhanced security but also avoids too much friction at the buying stage for most of your genuine customers.

Other common fraud detection tools include:

- validation services (e.g. email verification, credit history check, card verification number, geographic indicators)
- company data/customer history (e.g. customer order history, blacklists and white lists, fraud scoring models, and velocity tests)
- multi-merchant data/purchase history (e.g. shared negative lists and identity morphing)
- purchase device tracking (e.g. geolocation information, device fingerprinting)

Source: List of fraud detection tools supplied by Cybersource 'Online Fraud Benchmark Report', 2017

Top 10 fraud detection tools most adopted by North American businesses

Source: CyberSource 2017 Online Fraud Benchmark Report

3. ONLINE FRAUD PREVENTION

Automated fraud detection, as described above, is a flagging system. Fraud prevention, on the other hand, is all about being proactive. In other words, it's stopping a fraudster in his or her tracks. There is a host of ways of doing this, some are more sophisticated than others. These include:

- manually checking orders flagged as suspicious by your fraud detection software
- using a "trust mark" security service on your e-commerce site to scan your systems every day for malware, viruses, and hacking attempts. This is a little bit like having a burglar alarm on your house. It doesn't offer 100% protection against crime, but it does make you much less attractive, and hopefully the criminals will move on to a more easily-accessible site.
- Implementing 3D Secure, which provides an additional online authentication step during the ordering process. The user is asked to enter the password known only to the bank and the customer. Well-known brands of 3D Secure include Verified by Visa, MasterCard SecureCode and American Express SafeKey. The flipside is that it greatly reduces conversion because many customers don't know their password and they don't like the extra steps in the checkout process. What's more, it's not available all over the world.
- Using an Internet Protocol (IP) intelligence solution that deploys several methodologies in a layered approach to analyse your data. By implementing this, you know that if a hacker manages to overcome one of your security hurdles, he or she will be faced with another hurdle to jump over, and then another. You can have a whole series of hurdles.
- Using different solutions and technologies to track fraud attempts via online and mobile channels separately. These remote channels have different security issues, so what works well for one doesn't necessarily work for the other. If you monitor them together, you could miss something significant.

According to the '2016 True Cost of Fraud Study' by LexisNexis, more than 80% of large e-commerce/m-commerce retailers use at least one or more fraud protection solutions. Most use between five and six fraud prevention solutions.

It goes on to say that merchants who do best in fighting fraud are the ones who rely on a

multi-layered approach to fraud mitigation solutions. By layering the processes of identity verification, identity authentication and transaction risk assessment, the merchant experiences fewer false positives and fewer successful fraud attempts than those who don't adopt a multi-layered approach.

Conversely, the same findings show that merchants who use multiple solutions, but not in a layered approach, experience more false positives and more successful fraud attempts as those who use very few solutions.

Top 10 fraud detection tools most adopted by North American businesses

Source: CyberSource 2017 Online Fraud Benchmark Report

4. ONLINE FRAUD ELIMINATION

The elimination of fraud is not something that most vendors of payment gateways offer. Using a payment gateway that guarantees your payments can be compared to taking out an insurance policy. If you incur a chargeback, for example, it will be eliminated.

In other words, you'll receive 100% of the income that you've earned. For merchants who operate in in a high-risk environment, this is surely the ultimate solution.

How can Alphacomm Solutions help you mitigate and eliminate payment fraud?

Alphacomm Solutions gives your customers a safer, faster way to pay, whenever and wherever they want. At the same time, you get to transfer all the risk of fraudulent online payments to us.

Our full range of payment and security capabilities includes a top-of-the-line white-label payment platform that gives you 100% uptime and can handle large volumes of data.

If you need to be guided through all the fraud detection, prevention and elimination options open to you, we have a team of fraud protection experts always on hand. Whether you're an e-commerce, m-commerce and mobile point-of-sale merchants, we've got a solution for you.

Finally, we're one of the few companies in the world that will guarantee your online payments.

Yep! We've got you covered.

If you found this article informative, please share it with your colleagues.
If you'd like to chat to one of our experts about your payment fraud concerns, please give us a call on +31 10 7989 501.

About Alphacomm Solutions

Alphacomm Solutions is a global partner in all top up, reminder, dunning and payment challenges. We just hate missed revenue.

With that in mind, we offer a unique full service payment solution and 100% fraud protection. We turn complex payment challenges into simple solutions for our partners.

Thanks to our 100% payment guarantee you don't have to worry about any fraud risk any more. Our solutions boost your revenue, bring maximum customer satisfaction and increase loyalty. Plus, we deploy a business model where your success is our success. Once you decide to use our endorsed branded products & services, we can have them up and running within weeks.

About the author

Huub Sparnaay
Founder Alphacomm Solutions

I started this company in 1997 as a provider of telecom hardware for large telecom companies worldwide. During the following years, I adjusted the business model to developments in the market. The result is Alphacomm Solutions, a service provider fully focused on delivering payment solutions to large B2C organizations.

With over 20 years of experience as entrepreneur, I'm focused on building companies and making them work. I love to challenge the status quo and to grow things. As such, I'm focused on new business, scale up and strategy.

I also have two other companies: Alphacomm Digital Commerce, a sister company of Alphacomm Solutions, an online international supermarket for digital goods. And BarrelQ, a manufacturer of oil drum bbq's that challenge the not so cool Weber's.