Protecting your bottom line from online credit card fraud

Industry analysts estimate the annual cost of online credit card fraud to be as much as US$60 billion. Depending on the type of transaction and industry, recent research estimates anywhere between 3% and 20% of online orders are fraudulent, with costs adding up to 10% of gross online revenue. This poses a significant risk to merchants who are solely dependent on credit cards as their primary method of online payment.

You can't look your online customers in the eye

Unlike face-to-face transactions, all credit card payments that take place online are virtually invisible, labeled in the industry as "Card Not Present" (CNP) transactions. The retailer can neither physically verify the presence of the card, nor the cardholder, which opens the door to fraudulent transactions, resulting in disputed transactions and charge-backs for you, the online merchant.

Additionally, the problem with credit cards is that authorisation does not guarantee payment. It only confirms that the card being used on your site has not been reported lost or stolen and that there are sufficient funds available, nothing more. That makes your business susceptible to the risk of bad debt, which means you end up paying the high price of fraudulent transactions.

Fraudulent credit card activity can originate from identity theft or customer data hacks on your site and anything in between. Left unmanaged, these threats end up hitting your bottom line.

The high price of fraud

The changing online environment together with the push to enter newer, more lucrative markets leaves credit card dependent merchants open to serious financial loss. Fraud, bad debt and identity theft plague the online retail marketplace costing merchants and consumers billions of dollars every year. And when those fraudsters are hitting you from other countries, it is either impossible or cost-prohibitive for you to do debt recovery, so kiss the money goodbye.

But, as every merchant knows, credit cards are a single-source payment mechanism that offers consumers instant, everywhere convenience. The question then becomes: how do online merchants leverage the core strengths of credit cards while mitigating the associated risks of fraudulent activity?

Three ways to protect your online business

There are a couple of different approaches you can take to manage the risk of fraud and bad debt, each with its own costs and benefits:

1. Keep up with ever-evolving credit card security features.

   To combat CNP fraud and disputed transactions, credit card companies recently introduced 3-D Secure™. Also known as a technical trust chain, 3-D Secure™ is an authentication protocol that requires cardholders to enter a user-generated PIN or password to verify their identity and validate the transaction. Online shoppers who wish to use 3-D Secure™ must register for this additional security feature through their card issuer.

   Any e-commerce business would be keen to adopt 3-D Secure™ because it shifts responsibility away from merchants back to the cardholders and credit card companies, thus eliminating the risk of "cardholder unauthorised" charge-backs for merchants. This can mean millions of dollars to some companies and simply peace of mind for others. The one undisputed fact is that these security enhancements boost customer confidence, which can in turn increase spending activity at your site.

But as with any new product, there are some constraints that merchants and credit card companies need to address before 3-D Secure™ can truly deliver. Dubbed by thee-commerce industry as “the conversion killer,” the biggest obstacle to3-D Secure™ is the additional authentication window that has become a common customer abandonment point. Beyond this, programregistration requirements vary by region—from merchant registration in Europe to merchant, consumer and card issuer registration in North America. Add to this confusion a generally low consumer adoption rate and suddenly a merchant’s eligibility for liability protection is somewhat limited.

2. Build identity checking and real-time fraud monitoring systems into your application.

From country profiling and identity verification to pattern matching and transaction monitoring, if you opt to accept credit card payments on your merchant site, the risk is entirely yours. Over the next 3–5 years, the single most important element in fraud detection and prevention is going to be the identification of real-time behavioural profiling. To protect your business from the risks associated with credit cards, you’ll need to build a comprehensive fraud mitigation program which requires establishing business rules, transaction processing, identity verification, KYC (Know Your Customer) and data security practices.

Here are just a few items you’ll need to consider before building your very own risk mitigation program:

- Identity verification using online and offline sources of identity information, including name, age, address and contact information
- Security policy development including PCI compliance, network security, data protection and encryption
- Anti-money laundering controls
- Risk profiles for your markets based on geographical region and business type
- Business rules to filter out suspicious transaction behaviours
- Cross-organisational training, especially for frontline Customer Support Representatives (CSR) to catch suspicious, anomalous or false information and activities

3. Rely on third-party payment processors with indemnified funds to assume the risk for you.

More and more merchants are opting to use external payment processors to handle their credit card payments. Today, e-wallets are gaining momentum because they ensure that your customers benefit from the convenience of credit cards without you having to take the risk of bad debt and charge-backs.

Merchants integrated with these e-wallet services benefit from comprehensive identity verification, transaction security, indemnified funds and increased consumer confidence, which all turn into dollars on your sites.

The safest way to pay

Today, over 100 million consumers use an e-wallet to shop online. As a virtual wallet for online consumers, an e-wallet is a next generation e-commerce solution that allows a user to transact with online merchants. Known as one of the safest and quickest ways to pay online, an e-wallet provides peace of mind for both the consumer and the merchant.

All e-wallet providers must be regulated and authorised as e-money issuers by a governing financial regulator in order to operate in the EU and most other countries. As a regulated entity, e-money issuers must fulfill all KYC and identity verification requirements, which protect your business from the risks of transacting with unknown, remote customers.

Some e-wallet providers also offer 100% indemnified funds, further shielding you from the risk of bad debt problems from CNP disputes and related charge-backs.

Partner to protect your business

Credit card fraud and identity theft pose a major threat to the success of your online business. The best mitigation approach to online credit card fraud is to partner with a reputable e-wallet provider that offers indemnified funds. This not only eliminates your fraud loss risk, but it also proves to your customers that you are serious about providing them with secure and simple ways of transacting on your site.

Learn more at: www.web-merchant.co.uk

Web-Merchant Services Limited
+44 (0)845 475 3540
info@web-merchant.co.uk