Effective Fraud Management for High Chargeback Risk Industries
## Contents

| 01 | Executive Summary | 02 |
| 02 | Evaluating your Industry’s Chargeback Risk | 03-06 |
| 03 | Negative Impact of High Chargeback Risk on Your Business | 07 |
| 04 | Common Misconceptions when Reacting to Intensified Fraud Attacks | 08-10 |
| 05 | Effective Fraud Management for Greater Sales and Business Growth | 11-15 |
| 06 | Conclusion | 16 |

---

### 02 Evaluating your Industry’s Chargeback Risk

- Intangible or Tangible Goods
- Delivery Method
- Resale Value
- Transferability
- Business Nature

### 03 Negative Impact of High Chargeback Risk on Your Business

- Direct chargeback loss
- Lack of Focus on Core Business Competencies
- Losing Payment Methods
- Intensified Coordinated Attacks
- Unlimited Losses

### 04 Common Misconceptions when Reacting to Intensified Fraud Attacks

- Limiting Order Amounts
- Requesting Additional Information
- Multiplying Identity Checks
- Reducing Payment Options on Web Store
- Ineffective Fraud Verification

### 05 Effective Fraud Management for Greater Sales and Business Growth

- **A Protected Business is a Growing Business:** Key Factors to Effective Fraud Management
  1. Positivity Weighs as Much as Negativity
  2. Automated Verification Topped with Manual Review
  3. Protection Should Entail Growth
- **Managing Fraud in Any Online Industry:** Minimize and Optimize
  1. Comprehensive and Flexible Solutions are Essential to Minimize Fraud
  2. Optimizing Risk to Achieve Business Growth
Executive Summary

Fraud is a constant menace to any online business, and keeping fraud rate to a minimum level is still one of the biggest challenges merchants must overcome. This battle against online fraud is especially relevant for certain industries, in which a specific, relatively risky business model intensifies the number of fraud attacks, thus preventing them from achieving growth.

In this report we intend to help merchants that have this specific business model to understand the reasons why their businesses are more likely to be targeted by coordinated fraud attacks. We will also simultaneously analyze the negative impact these attacks have on online businesses. We will then depict the most common, yet mistaken, reactions to this intensified attacks scenario, and their effects on business growth.

Finally, we will share some recommendations for an effective fraud management strategy that can help online businesses mitigate considerably the negative effects of coordinated fraud attacks. We will also explain the importance of adapting an appropriate fraud protection tool to the special fraud requirements of these businesses in order to optimize risk and achieve growth.
Certain online businesses are typically unaware that their business models attract a higher number of coordinated fraud attacks, and they tend to take these attacks as a normal consequence of doing business online. The truth is that some industries are more likely to chargeback risk than others. We have compiled the most common features of these business models so you can determine if your business is among them. It is important to highlight that businesses do not need to have all the features listed below, but adjoining to even one or two might get the business model labeled with a generic “high-risk” by some industry’s stakeholders, mainly the payment service providers and fraud protection suppliers, which could thus negatively affect the business’ ability to grow. Evaluating your industry’s chargeback risk might be crucial to attain real business growth.

The features common in the industries where chargeback risk is high are categorized as follows: intangible goods, delivery method, resale value, transferability, business nature and third-party reseller.

A. Intangible Goods
High chargeback risk industries are characterized by dealing only with intangible goods. Traditionally, intangible goods are associated with the gaming sector, an online segment whose list of intangible goods includes items for games, virtual currency and game-related services, such as power leveling or game account creation. In short, this list typically contains goods and services that can solely be used in the virtual world in a given game. However, with the widespread use of the Internet and the introduction of new, technology-led lifestyles, the intangible goods list has been enlarged to now involve a wide array of online segments.

- **Game industry**, including game items and services, key and game time cards, accounts resellers, game downloads and game-related auction sites
- **Prepaid telecommunications**, including prepaid phone cards, Internet access cards, mobile cards
- **Gift cards and eVouchers**, including both the suppliers of gift cards and the merchants providing this service to their clients
- **Downloadable software**, including updates and apps, a growing industry from the widespread use of smartphones
- **Music and films**, including iTunes cards, codes for legal download of music and films
- **Ticketing**, including sports events and other leisure activities, such as cinema, theatre, concerts, museums and tourist services (entry tickets to historic/cultural sites)
- **Travel**, including air ticketing, tour packages, hotel and tours booking
- **Prepaid debit and credit cards**, including suppliers and resellers of these payment methods to online shoppers who lack a bank account or wish to better control their online expenditures by using debit cards with a prepaid limit
- The file sharing and hosting industry
• **e-Learning and translation services**, including e-courses, proofreading and editing

• **Browser** and **social networks**

• **Data mining** companies

If your industry is not on the list above, but it meets one or more of the features described in this section, that means your industry’s chargeback risk is high; in fact, the risk is so high that it might mean business closure for those merchants unaware of their industry’s needs.

There is no doubt that the intangible goods sector is growing in every country, regardless of the market’s e-commerce maturity. The following figures from 2011 leave no doubt about this trend. According to the North America B2C E-Commerce Report 2012 by the Hamburg-based consulting firm YStats.com, “digital content and subscriptions” was the fastest growing sector in the United States in 2011. This retail category includes digital downloads of music, TV, movies, e-books, and applications. In 2011, the value of virtual goods purchased in the United States reached over US$2.3 billion, with gamers spending an average of US$64.00 each. In the U.S., 35% of online consumers acquired a virtual good in 2011, a 50% increase compared to 2010.

The intangible goods sector in Germany is growing at one of the fastest paces in Europe. Media (image and sound) were the top two best-selling sectors in 2011, totaling US$3.7 billion of all the online sales. Additionally, digital services continue to drive interactive trade figures: ringtones, apps and software accounted for an additional US$253 billion in Q3 2011, according to bvh, the German association for distance and online selling. Most of the figures found for the intangible market in the United Kingdom refer purely to online gambling and casinos.

According to figures issued by the UK Gambling Commission, gambling represents the largest market within the industry with a 53% share.

In China, most of the intangible goods market revolves around online gaming. Figures published by the Chinese Ministry of Culture state that the online gaming market reached US$7.4 billion in 2011, and it is expected to exceed US$15.9 billion by 2015.

Online businesses trading with tangible goods are also likely to be targeted by fraudsters. The main difference is that tangible goods are physically delivered, thus merchants can verify the buyer’s identity before shipping the goods and perform further verification checks, as these goods are not expected to be immediately delivered.

### Value of Online Intangible Goods in 2011 in Key Markets (all figures in billion USD)

- **China**: 7.4 billion USD
- **Germany**: 3.7 billion USD
- **US**: 2.3 billion USD
B. Delivery Method
Intangible goods are usually delivered electronically. Electronic delivery can be performed in different ways. We will focus on the three most typical ways of electronic delivery. The first way of delivering intangible goods is by sending them directly to the e-mail address the buyer enters into the merchant’s website. For example, a CD key code for a massively multiplayer online role-playing game (MMORPG) provided by an online game supplier can be delivered using this method.

The second way of delivering intangible goods is by sending a link to the customer’s e-mail address. The customer can then access the link and download the goods. This is the case with business reports sold by intelligence companies, for instance.

Third and last, intangible goods can be delivered by using “the flashing codes”, whereby a screenshot with the code is uploaded to the merchant’s website, and the customers logs in after purchase to access the code. This is usually the case with prepaid phone cards or e-vouchers. Some merchants also choose to flash the code that grants access to the purchase on the screen.

The risk involved in these ways of delivering can be reduced by validating the e-mail address entered by the customer. Validating the e-mail requires additional time and slightly delays the delivery, which is why an increasing number of merchants choose not to validate their customers’ e-mail addresses, thus unintentionally adding risk to the transaction.

Whichever way merchants choose to deliver their intangible goods, the exchange of ownership for electronically-delivered intangible goods takes place within seconds, making it extremely difficult to trace these goods.

Conversely, tangible goods are physically delivered, thus requiring the action of third-party service providers such as shipment companies that can issue a delivery proof (proforma invoice, acknowledgment of goods receipt, etc). Intangible goods do not require these services, and merchants trading with intangible goods find it more difficult to prove an electronic delivery.

C. Resale Value
Intangible goods tend to retain much of their original value once purchased, and this guarantees their high resale value, as they can be resold at almost their original price in the shortest time possible after purchase. This is an optimal way for fraudsters to obtain financial gain while remaining undetected. A good example of an intangible good with high resale value would be an e-gift card to be redeemed at the web store of a well-known department store.

It is important to note that, despite their high resale value in their virtual world, some of these intangible goods are regarded as worthless in the physical world. For instance, online games players must spend both time and money in order to obtain certain items of popular online games. This increases their popularity and retains their original value in the virtual world among fellow players. Merchants dealing with this type of goods are often unprotected by law, since few courts or authorities will acknowledge the value of these items in the real world in case of loss, regardless of whether or not the loss is intentional.

D. Transferability
Most of the intangible goods or services available can be used without requiring personal data, which makes them easily transferable. This guarantees fraudsters a seamless resale process and makes it more difficult to trace the fraudulent order, while adding anonymity to the fraudster. Example: iTunes cards or tickets for major sports events.
E. Business Nature
High-risk businesses are usually operated online-only, as compared to hybrid businesses that might generate part of their income from their bricks-and-mortar lines of business. It could be argued that all merchants selling online are likely to suffer fraud attacks. Truthfully, every online business entails the risk of fraud. However, the risk rate intensifies when you add any of the features described above.

Card-not-present transactions are essential to e-commerce. Credit cards are wide-spread, easy to use and consumers perceive them as a fast and secure payment method to conduct their online shopping. Merchants’ perception of this payment method might be slightly different. In 2011, 65% of all card fraud in the UK (US$341.9 million) was due to card-not-present fraud, while US$34.8 million were due to card ID theft, according to Fraud The Facts 2012, by Financial Fraud Action UK. The total fraud losses on UK-issued credit cards in 2011 represented US$527.8 million. These figures represent the fraud loss in Europe’s most card-oriented market. The joint actions between banks, card acquirers, consumer associations and government agencies have made it possible for the UK to decrease credit card fraud by 7% in 2011 for the third year in a row. These joint actions and their positive results are encouraging, but merchants should not be complacent and only rely on these actions to keep their businesses protected. An effective fraud management is vital to supplement these joint projects.
Direct chargeback loss
As explained above, businesses dealing with intangible goods that are delivered electronically face higher chargeback losses than any other online businesses. The intangible goods segment is growing in turnover and number of businesses, most of which are too new or too small to stay well informed about the risk of fraud. Fraudsters thus find a favorable situation with an increasing number of poorly-protected targets. Merchants’ direct chargeback losses are understood as the value of all those orders that merchants processed but that were indeed fraudulent.

Lack of focus on core business competencies
Upon realizing how much lost revenue was generated by the direct chargeback specified in the paragraph above, merchants start investing time and resources in an attempt to reduce the amount of fraudulent orders in their online sales. In spite of merchants’ efforts, online fraud is increasingly sophisticated and fraud schemes evolve as rapidly as fraud verification systems develop. Most merchants find it challenging to keep up with that fast-evolving pace, and they end up focusing totally on reducing fraud and chargeback, overlooking entirely vital business aspects that aim at growth.

Losing payment methods
Online businesses that face a high chargeback rate risk might not be able to offer the desired payment method on their websites. Fraudsters are aware of which payment methods are easier to attack, and target those methods to maximize their gains.

As a result, merchants decide to stop offering that particular payment method, while trying to divert customers to presumably safer options. Payment service providers might also impose extra charges for those businesses with high chargeback rates. This measure usually deters merchants from using a defined payment method and, by extension, the services of that payment provider.

Intensified coordinated attacks
Fraud is more than chargeback these days; fraudsters function in globally-connected organizations, and their attacks are increasingly sophisticated and difficult to detect. Merchants who are often targeted by coordinated actions find it hard to recognize the pattern behind the attack: by the time they do, the harm might already be done and a new attack based on a different fraudulent scheme could be on the way. Merchants must realize that their businesses are constantly under attack by a range of fraud techniques much wider than what they should cope with.

Unlimited loss
The high chargeback risk involved in these businesses does not only imply the chargeback loss itself, but, as described in the points above, it also includes higher risks that all lead to customer and sales losses, extra spending and misuse of resources, as well as to neglect important areas for business differentiation. This unlimited loss, borne especially by businesses where the chargeback rate is high, entails the biggest risk of all: business closure.
Common Misconceptions when Reacting to Intensified Fraud Attacks

Merchants’ most common reaction to the intensified and recurring coordinated fraud attacks is to automatically tighten the verification rules for accepting orders on their websites. Fraud attacks usually follow a specific pattern but finding out the algorithm that generates the attack usually takes some time. Merchants fail to realize that every attack is different, and there is no one-size-fits-all approach to protection against these attacks. The most common actions merchants tend to perform to reduce online fraud are the following:

**Limiting Order Amounts**
Merchants might find out that orders coming from a certain server or IP Address result in chargeback, so they consequently block and do not process all those orders. In an attempt to avoid any new attacks, a common practice among merchants is to limit the amount of daily orders that a customer can make, the daily amount that a customer can spend in several orders, and the amount per order. These procedures might minimize chargeback rate initially, but they will not deter fraudsters from attacking the merchants’ websites. What is even worse, blocking or limiting orders on the basis of simple suspicion might result in the rejection of genuine customers.

**Requesting Additional Information**
As mentioned at the beginning of this report, most intangible goods only require a valid e-mail address to be delivered, and it is increasingly common for merchants to accept orders without requiring customers to have a preregistered account at the merchant’s website or even to accept anonymous orders. When the chargeback rate increases, merchants react by requesting additional information from customers, such as proof of customers’ identity or residence. Customers failing to submit the requested information will not see their orders processed. Needless to say, not every customer is willing or even able to submit what they probably consider to be sensitive information to a merchant, especially during a first-time purchase. In the case of recurring customers, the insult factor is quite high, and customers might take their purchases to a competitor’s website.

Besides, even assuming that customers submit all the requested information, how can merchants be sure that the information provided is not false? With identity fraud on the rise, it is becoming more and more difficult for merchants to distinguish a genuine order from a fraudulent order made with false or stolen, yet extremely reliable, information. Verifying orders using only identity checks does not derive conclusive results, and this verification tool can only be useful if combined with other tools.

**Online criminals have illegally traded 12 million pieces of personal information between January and April 2012.** Unfortunately, 2012 has seen two major security breaches to prove this growing trend. In March 2012, card processor Global Payments reported a massive security breach compromising approximately 50,000 North American Visa and MasterCard holders. Fraudsters managed to obtain no less than 1.5 million credit card numbers. In June 2012, LinkedIn, the social network for business professionals, disclosed that over 6 million customers’ passwords had been hashed (encoded). These passwords give access to valuable personal data stored by LinkedIn. Even though the company reacted promptly and assured compromised passwords had not been used to access accounts, it is a matter of time until those data are used for fraudulent purposes.
Multiplying Identity Checks
Another example of a common reaction to reduce chargeback, especially among those merchants with higher business volumes, is to multiply the number of identity checks before completing the checkout process. This procedure adds friction to the checkout process, and merchants following this practice might see their chargeback rate reduced, but they will surely see their cart abandonment rate increase.

Reducing Payment Options on Web Store
Some payment options, such as credit cards, are more fraud-prone than others. When merchants analyze the attacks to their websites and realize which payment method has registered the highest chargeback rate, it is relatively normal to divert customers to other payment methods or even to stop offering the payment methods that were under attack. Reducing the number of payment methods in the website also reduces the number of potential customers. Limiting the payment options in a website to only those methods considered “safe” against chargeback might also bring a reduction in the sales volume.

Fraudsters will surely tend to target those methods that are considered less safe, but that does not mean that merchants should delete them from their web stores.

It is important, therefore, for merchants to understand each payment method, and, above all, to identify what is the perceived risk is in every method. Understanding how those payment methods work allows merchants to adapt their verification solutions and optimize the risk involved without having to give up on customers.

For instance, credit card transactions are probably the best example of a perceived “risky” payment method. Credit cards are one of the most widespread payment methods among customers.

What’s more, popular eWallets like PayPal, Skrill and Google Checkout are also connected to customer’s credit cards, which means that merchants who fail to offer credit card transactions potentially lose customers. Verification checks are done before accepting any transaction; in the case of direct credit card processing, the customer is driven to a different website where the usual verification tests are completed, while in the case of credit card transactions done via eWallets, the verification tests can be done in the merchant’s website. Regardless of where the verification tests take place, what is the risk implied in any of those transactions?

Due to the popularity of direct credit card processing and the high possibility of chargeback in these transactions, the world’s largest card acquirers developed specific technology to confirm the holder’s identity before completing checkout. Most of the merchants adhere to these schemes, the most popular of which being Card Verification Number or CVN tool. This tool directs customers to the acquirer’s website and requests a code that is often found on the back of the card. Another popular verification tool is the one called One-Time-Password (OTP) by which customers receive a code via an SMS to the registered mobile phone. Customers then introduce the code into the website to complete checkout. Even though most merchants use these tools in their web stores, very few of them would rank them as truly effective to fight against chargeback. Merchants know that it is easy and cheap for fraudsters to obtain full credit card details, including codes, on the black market. The OTP tool can equally be subject to fraud attacks; fraudsters can gain access to the code and make fraudulent use of the credit card.

When it comes to indirect card processing (card transactions done through an e-Wallet), merchants have part of the customer’s information.
However, this does not mean that the information merchants can access is not fake and that it belongs to a genuine customer. **Coordinated fraud attacks targeting credit cards are very difficult to detect**, if merchant’s verification system is not up to date, or if it lacks the sufficient verification tools needed to detect such attack. The key to reduce fraud attacks lies not in the payment method but in the fraud verification system itself. Merchants should not be deterred from offering a specific payment method on the grounds of chargeback risk, high fees or likelihood of unauthorized transactions. Being aware of the risks of each payment method and relying on the appropriate verification system are the essential points to reduce fraud effectively without reducing payment options on the web store.

**Ineffective Fraud Verification**

The previous points indicate that fraud verification is one of the key aspects merchants should bear in mind when reacting to intensified coordinated attacks. When facing these attacks, merchants tend to just focus on the chargeback loss and to overlook other aspects that ineffective fraud verification inherently brings to their businesses. Here are some of them:

- **Time spent in verifying a chargeback**: fighting chargeback can be a lengthy process, and the success rate tends to be proportionally inverted to the amount of time spent by merchants and verification staff trying to sort out the chargeback with payment gateways, banks and even final customers.

- **Redefinition of fraud verification tools**: as a response to high chargeback rates, merchants or their fraud protection suppliers tend to apply restrictive thresholds to their tools, resulting in more orders, both fraudulent and genuine, being rejected. This approach is detrimental to the business in the long run, as it severely hampers sales by deterring genuine customers from buying and does not stop fraud attacks from the root.

- **High fees**: high chargeback rates are often penalized by banks, card issuers and some payment providers via higher fees for merchant meant to cover the expenses generated by potential chargebacks. Should the chargeback rate be too high, merchants might even risk having their accounts suspended.

In this sense, it is important to be aware of the true cost of verification. Fraud losses involve much more than incurring chargeback loss these days. Merchants must be aware that verifying orders entail “hidden” costs, such as the loss, financial and reputational, associated with genuine customers being wrongly rejected and/or customers abandoning orders for long verification wait times. These “hidden” costs tend to be overlooked. All those costs, when added to the normal maintenance costs of having an appropriate verification system and staff, make the final cost of verification much higher than what was initially budgeted. What’s more, overlooking these costs might result in merchants spending more resources in combating fraud than what they are saving.

Fraud attacks are growing in frequency and intensity, and the industries described in the first part of this report are the fraudsters’ preferred targets. All of these common reactions to coordinated attacks bring customer loss, as explained in this section, and they all share one underlying element – failure to use effective fraud management to achieve business growth.
Effective Fraud Management to Greater Sales and Business Growth

A Protected Business is a Growing Business: Key Factors to Effective Fraud Management

Fraud management is a critical aspect for every online business. Online merchants from any industry must be aware that fraud management inherently affects the customer experience: the choice of a fraud management solution reflects the company’s long-term objectives, branding, and reputation, and it is intertwined with the company’s profitability.

The protection against online fraud is much more than just blocking every potential fraudulent transaction. It is vital to understand that the chosen fraud protection solution should consider all relevant factors of effective fraud management. Given the business nature that dominates the high chargeback risk industry, these relevant factors can be summarized as follows:

1. Positivity Weighs as Much as Negativity
Detecting threat is important for early fraud detection. Having a detection system tuned to detect unusual activity that can be related to unauthorized transactions does help to reduce the number of fraudulent orders, but it is just not enough. Simply reacting to negative aspects, such as device reputation, multiple IDs or mismatching information, among others, might increase the rejection rate. The costs associated with an increase in the number of orders rejected, many of which could potentially be genuine orders, can be much higher than the chargeback avoided. Rejecting orders based purely on negative aspects becomes, in fact, detrimental for online business in the long run.

Positive aspects of an order should be considered as much as negative aspects and should be taken into account to assess the real risk of fraud, ensuring that the highest number of genuine orders is accepted.

2. Automated Verification Topped with Manual Review
Automation should be a priority to secure both high sales volume and customer experience in any web store. It is especially relevant in the case of virtual merchants, whose customers expect their orders to be electronically delivered right away upon payment confirmation. Long waiting times for confirmation or delivery can cause lost sales, not to mention reputational damage done via negative reviews of the merchant’s website.

Is manual review out of question for merchants with a higher frequency of fraud attacks? Not quite. By adding thin layers of human verification, manually reviewing orders ensures only fraudulent orders are effectively blocked. Nevertheless, it should be done by professionally-trained officers who can assess the optimal risk per return tradeoff in a suspicious order.

Positivity vs. Negativity: Success Case
Focusing on positive and negative aspects helped a leading, online prepaid phone service provider achieve an increase of +40% in new customer acceptance rate. The merchant has experienced a high amount of fraudulent transactions before due to the existence of a black market specialized in reselling the prepaid cards and all related products on the merchant’s website. By implementing CashShield’s real-time automated verification system, merchant increased its acceptance rate by 25% only 30 days after implementation. CashShield analyzes both the positive and the negative elements in an order and is, thus, capable of optimizing the order acceptance rate. Moreover, the automation of the whole verification process leads to a growing customer satisfaction, and a considerable increase in the sales volume generated by a popular payment gateway.
Manual verification is especially important in those online businesses accepting direct credit card transactions. As explained in the previous section, verification tools like Verified by Visa or MasterCard’s 3D Secure Code cannot distinguish exactly between genuine and fraudulent orders. When the tests fail, the order is lost, regardless of the reason that caused the authentication to fail. Resuscitating those failed orders by manually reviewing them means the merchant is preventing the customer from abandoning the cart and moving to a competitor’s website, even if accepting that order means taking some risks for borderline orders. Manual verification does mean longer processing times for customers, but it also increases significantly the order resuscitation rate, which eventually leads to business growth in any industry.

Engaging in a fraud protection solution means a vital aspect of online business, fraud management, is entrusted to a provider that understands the merchant’s business nature, needs and corporate objectives. Only by aligning to a provider that walks in the same direction can merchants ensure that their growth objectives will be met and that their fraud protection needs will be covered.

### Automation, Rejection and Resuscitation

In 2011, 56% of the merchants surveyed in *Cybersource’s Online Fraud Report 2012, 13th Edition* used an automated screening system. The same survey reveals that the merchants surveyed rejected 2.8% of orders due to suspicious payment fraud, a trend that has been increasing since 2009. In 2011, 75% of these merchants also reviewed manually 27% of the orders reaching their websites, compared to 2010 when 72% merchants reviewed manually 24% of the orders.

### 3. Protection Should Entail Growth

If all business areas are planned to attain business growth, fraud management should not be an exception. Fraud protection should focus on growth rather than on threat detection: thus, merchants must ensure their fraud detection providers share their corporate interests. This includes constantly redefining risk thresholds to quickly adapt to new fraud schemes and customizing the solution to the merchants’ needs.

**3. Protection Should Entail Growth**

Engaging in a fraud protection solution means a vital aspect of online business, fraud management, is entrusted to a provider that understands the merchant’s business nature, needs and corporate objectives. Only by aligning to a provider that walks in the same direction can merchants ensure that their growth objectives will be met and that their fraud protection needs will be covered.

**Automation, Rejection and Resuscitation**

In 2011, 56% of the merchants surveyed in *Cybersource’s Online Fraud Report 2012, 13th Edition* used an automated screening system. The same survey reveals that the merchants surveyed rejected 2.8% of orders due to suspicious payment fraud, a trend that has been increasing since 2009. In 2011, 75% of these merchants also reviewed manually 27% of the orders reaching their websites, compared to 2010 when 72% merchants reviewed manually 24% of the orders.

**Managing Online Fraud in Any Industry: Minimize and Optimize**

Once the relevant factors of accurate and effective fraud management have been analyzed to ensure online businesses aim at growth, it is time to assess which is the best way to keep businesses protected. A misleading idea among merchants is that the best verification solution is the one that sweeps fraud out automatically. The truth about online fraud is that no single tool, when used alone, can effectively block fraud 100%. Actually, even when merchants use a combination of different verification tools, a reduced fraud rate might probably remain, since having no fraudulent orders at all often means that merchants are rejecting genuine orders. Any merchant rejecting genuine orders on the wrong basis should consider revising their approach to preventing online fraud.

**The good news for merchants is that a combination of several tools can efficiently minimize fraud rates and help them optimize the remaining fraud rate.**

Online businesses grow with online sales, and online sales make online fraud increase.

---

Losing Revenue to Fraud

According to *WorldPay’s Perfect Passenger Payments*, the airlines surveyed lost 1.5% of annual online revenue to fraud, and around 25% of the airlines have not implemented any fraud management or chargeback protection systems. Even though 29% of the airlines admit that fraud has increased, many of them issue tickets even to those orders that are suspected of fraud.

Managing Online Fraud in Any Industry: Minimize and Optimize

Once the relevant factors of accurate and effective fraud management have been analyzed to ensure online businesses aim at growth, it is time to assess which is the best way to keep businesses protected. A misleading idea among merchants is that the best verification solution is the one that sweeps fraud out automatically. The truth about online fraud is that no single tool, when used alone, can effectively block fraud 100%. Actually, even when merchants use a combination of different verification tools, a reduced fraud rate might probably remain, since having no fraudulent orders at all often means that merchants are rejecting genuine orders. Any merchant rejecting genuine orders on the wrong basis should consider revising their approach to preventing online fraud.

**The good news for merchants is that a combination of several tools can efficiently minimize fraud rates and help them optimize the remaining fraud rate.**

Online businesses grow with online sales, and online sales make online fraud increase.

---

A publication by CashRun Pte Ltd. Copyright© 2012. CashRun Pte Ltd. All rights reserved.
Online fraud is, after all, an unavoidable part of e-commerce, and the right approach to help ease its effects on business goes through minimization and optimization.

1. **Comprehensive and Flexible Solutions are Essential to Minimize Fraud**

Each verification tool is specialized to protect merchants in just one area, leaving the rest of the areas open to fraud attacks. Most of the fraud protection solutions available these days only offer one or two verification tools. In order to determine which solution suits merchants better, it is necessary to analyze the current verification tools and their weak points.

Below is a brief summary of the tools and their flaws.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reverse Phone Checks</td>
<td>The results from these checks are only reliable in those countries/regions where registering phone numbers is common practice.</td>
</tr>
<tr>
<td>E-Mail Validation</td>
<td>E-mail accounts can be hacked by fraudsters, who use stolen identities to place fraudulent orders.</td>
</tr>
<tr>
<td>Device Fingerprint</td>
<td>Data compiled by Device Fingerprinting is insufficient to detect first-time fraudsters, and even in the event of a returning fraudster, a unique digital fingerprint might not always be attainable.</td>
</tr>
<tr>
<td></td>
<td>Additionally, orders done from public PCs (Internet cafés, hotels, airports, etc.) that have been already been used by fraudsters are automatically rejected, even if they are made by genuine customers.</td>
</tr>
<tr>
<td>Global Credit Databases</td>
<td>These are only useful in the event of friendly chargeback, since it is easy to check the customer’s credit history in the database.</td>
</tr>
<tr>
<td></td>
<td>However, global databases are not useful to detect unauthorized payments made with stolen credit cards or to detect fraud in anonymous purchases, an increasing trend in merchants’ practices worldwide.</td>
</tr>
<tr>
<td>IP / Geolocation Services</td>
<td>It is useful to locate a customer and the device in the real world, but in the case of merchants dealing with intangible goods, where no physical delivery or shipping address is needed, the information from these services is totally irrelevant for fraud detection.</td>
</tr>
</tbody>
</table>
### Phone Checks

Phone checks can be done via an outsourced, automated service, a call made by a verification officer or via an SMS sent to the customer’s phone.

Regardless of how phone checks are done, the results derived from them are inconclusive since fraudsters can have access to either the phone number or the device itself. Phone checks add friction to the sale process by increasing the insult factor to customer. Besides, with identity fraud on the rise, fewer customers are willing to disclose personal information including contact number when completing a purchase online, which will prevent merchants from being able to perform the checks.

### Card Authentication Schemes

Once again, fraudsters might have access to both the credit/debit card number and the CVV number, so a fraudulent order will be undetected.

Moreover, the increasing sophistication of fraud attacks has made these schemes an easy target for fraudsters, who have created similar looking pages and managed to phish the complete credit card details from the unsuspecting customers.

### Address Verification Tools

The results from this tool are ineffective for international orders. Also, customers having more than one card might have not updated their file with their banks or might have forgotten the address they used to apply for the card, not to mention orders placed by today’s world “global citizens” who might hold different cards with different banks in several countries.

### Fraud Detection Tools Provided by Payment Gateways

False positives orders are common within these tools, especially for merchants selling intangible goods, because the credentials to unlock an order are sent directly to customer’s e-mail, immediately after completing the checkout. Not only is it easy for fraudsters to place an order, it is also easy to unlock it.
Given the specifications of each tool as described above, minimizing fraud requires covering as many areas of specialization as possible, protecting e-business from potential fraud attacks. **Choosing a solution that combines as many verification tools as possible is the key to effectively block fraud.** The chances of detecting a fraudulent order are higher if the order is analyzed from as many attributes as possible. **This can only be completed with a comprehensive solution that combines several tools and draws a real and meaningful picture of the risk of fraud by weighing both the positive and the negative aspects of every order passing through the merchant’s website.**

Online merchants these days serve customers all over the world, which implies these websites offer an array of payment methods catering to the needs of every regional market.

This is the reason why fraud protection solutions should also be flexible, since certain payment methods are more chargeback-prone than others, and the risk thresholds should be adjusted accordingly and revised periodically. It is no secret that fraud schemes change as fast as fraud detection solutions evolve, which leaves merchants no choice but to keep up with the fast-paced race of the battle against online fraud. Business survival now relies on using a solution that can adapt, or better still, can foresee the changes in the fraud schemes.

2. Optimizing Risk to Achieve Business Growth

As mentioned earlier in this report, online fraud is unavoidable, so minimizing it with a comprehensive and flexible fraud protection solution is only the tip of the iceberg. **What lies underneath that solution is optimization of the risk of fraud faced by every successful online business.** The ability to analyze all the key considerations, including those positive attributes that tend to be undetected by merchants, provides business with a complete risk picture that helps weigh and assess the risk of fraud. It is this picture that allows businesses to make decision between the risk of chargeback and the risk of losing lifetime sales from a customer; blocking fraudulent orders is as important for business growth as taking the risk of accepting suspicious-looking orders that are, in fact, genuine. **Fraud management not only reduces the risk of fraud, it also aims at increasing a merchant’s profit rate, and that can only be achieved by incrementing the acceptance rate and keeping the business protected from common and new fraud patterns and attacks.**
06

Conclusion

Online fraud is an unavoidable part of online business. Within the online sector, those industries that deal with intangible goods delivered online with high resale value suffer from frequent and intense coordinated fraud attacks. The resulting chargeback rate from those attacks has very negative consequences to these businesses, and often translates into higher processing or verification fees from industry suppliers and rejection from payment providers.

Confused by the intensified attacks, merchants belonging to these industries often react by limiting those business areas which are more likely to attract fraud without realizing that these well-aimed reactions do not deter fraudsters’ attacks and might even generate unlimited loss for their businesses in terms of direct chargeback loss, customer or reputation loss.

Merchants dealing with intangible goods should be able to do business without any restriction in the payments or verification areas, and without facing higher fees charged on the grounds of their businesses nature. With the increasing sophistication of fraud attacks, it is essential to rely on a fraud verification system that can detect any fraudulent pattern and effectively block it without negatively affecting genuine customers.

About CashRun
CashRun was established in 2007 with the objective of supporting business’ needs for effective and affordable fraud protection solutions. Since establishment, CashRun has had tremendous success with key industries that are sensitive towards fraud, and continues to be at the forefront for e-commerce solutions. With strong global presence and partnerships, CashRun supports online merchants to develop and concentrate on their core business competencies while protecting against the risk of online fraud.

About CashShield
CashShield is an innovative and comprehensive one-stop risk management solution that analyzes the attributes from a wide range of information including customer, payment, device and network information.

- Risk scores and decisions are based on a risk management algorithm specifically designed to assess each of the key variables received and help each merchant achieve an optimized return per risk-level for their business.

- It provides real-time, automated verification with a unique 100% Chargeback Protection policy.

- It considers not only negative elements but also positive elements of an order thus minimizing the rejection of legitimate customers and optimizing order acceptance rate.

For more information, visit www.cashrun.com or email enquiries@cashrun.com