

A decorative graphic consisting of two overlapping shapes, one yellow and one blue, resembling a stylized paper airplane or a swoosh, positioned above the main title.

## Online Electronic Games

Global Fraud Prevention and  
Best Practices for Visa Merchants



# Overview

This document identifies common methods used by fraud rings to exploit online electronic game (e-game) merchants and provides best practices employed by the online electronic game (e-game) industry to combat fraud in the card-not-present (CNP) channel. The CNP sales channel for Internet and mail/telephone orders enables merchants to expand their reach to customers around the globe and increase sales revenue opportunities. Now recognized as the top acquired fraud type globally, CNP fraud presents significant challenges. Criminal exploitation has a direct impact on merchant revenues and operational costs. To effectively plan and organize an effective fraud mitigation strategy, merchants must remain abreast of fraud trends and best practices to help them combat incidents of fraud.

Among the top industries targeted by fraudsters is the online e-game industry. Typically, the fraud attacks against this industry involve fraudsters registering for an online e-game character and then purchasing character “upgrades” using fraudulent payment card account details. The fraudsters then resell the character upgrades (or even the entire character itself) at a discount to buyers using notices on web chats and auction sites. Payment is often made through virtual cash or other means outside the electronic payment environment.

Challenges unique to the online e-game industry include the difficulty of authenticating the actual user without imposing onerous registration requirements, and the difficulty of preventing (and tracking) the sale or transfer of characters or virtual character upgrades.

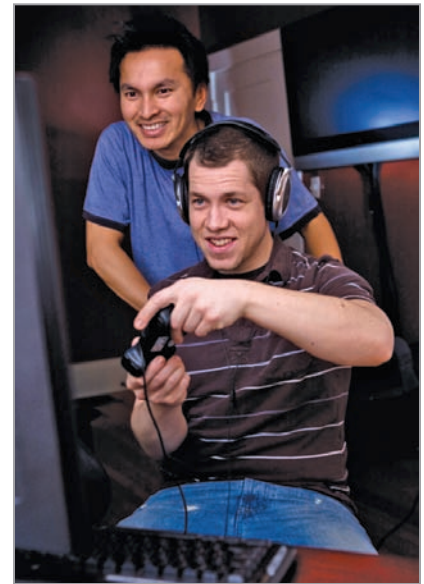
This document is to be used as a guide for new and existing e-game merchants. Whether you are just starting out in e-commerce sales or have already established a successful sales channel, this document will support your risk management capabilities and practices and help reduce your risk of CNP fraud within the e-game industry.

There is no single, simple solution to managing fraud risk. Rather, it is a continuous effort that involves a comprehensive, layered fraud reduction strategy. This approach combines the use of a variety of risk tools, strategies, and fraud controls that will mitigate incidents of fraud without restricting business development.

## E-game CNP Fraud Reduction Best Practices

This best practice guide compiles feedback from online e-game merchants that have successfully managed online fraud. In general, online e-game CNP fraud reduction best practices can be segmented into three continuous parts:

1. Establish strict user registration policies in which merchants validate users at sign-up;
2. Actively monitor the game environment to identify suspicious characters and suspicious credit top-up<sup>1</sup> activities;
3. Take strong, preventive action against identified suspicious characters and users to ensure that these identities are not used again in the future.



<sup>1</sup> Online e-game “top-up” term represents the purchase of online game virtual currency/credits using a Visa payment card account.

## 1. Strict User Registration

At the online e-game portal, gather sufficient information about your customers while also informing them of certain risk management requirements. Key best practice tactics at the point of user registration include:

### **Mandating customer registration.**

This should include submission of mandatory customer information such as name, contact details, e-mail address and date of birth.<sup>2</sup> A confirmation e-mail should be sent to the customer's e-mail address; the customer's account should only be activated as a result of the customer clicking on the activation link.

Customers' IP addresses should automatically be logged, allowing you to build comprehensive databases of both genuine "positive list" (i.e., customers that have been authenticated and well established to the merchant and do not generate fraudulent transactions), and "negative list" customers (i.e., those who are using fraudulent payment card accounts). All new registrants should be matched against the negative list database.

### **Utilize a suite of authentication tools.**

E-game merchants are encouraged to implement a comprehensive suite of authentication tools to make more effective transaction risk assessments and decisions. When used in a layered approach, tools such as Card Verification Value 2 (CVV2), Address Verification Service (AVS), and Verified-by-Visa (VbV) for CNP transactions can greatly reduce the incidence of fraudulent transactions and increase merchant profitability. However, it is important to note that no single risk tool should be considered a "silver bullet" against criminal exploitation.

- **CVV2** (a 3 digit code on the back of card) is a useful tool to determine if the user has possession of the physical card and will effectively detect fraudulent attempts using software-generated account numbers or situations where a card number was stolen, but the card remains in the legitimate cardholder's possession. E-game merchants should incorporate the CVV2 response codes into their overall transaction risk assessment process. "No Match" response codes coupled with other red flags may be strong indicators of a fraudulent transaction.
- **AVS** allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available in the U.S. and Canada. The United Kingdom also supports a domestic version of this service.
- **VbV** is an online service designed to secure Internet purchases by authenticating the cardholder's identity at the time of purchase. Additionally, VbV-enabled merchants are also protected from chargebacks for Reason Code 83 (Fraudulent Transaction—Card-Absent Environment) even when the cardholder and/or the issuing bank are not participating.



### **Implementing random character validation at customer registration.**

Random character validation should be implemented to prevent fraudsters from using a computer to automatically generate large numbers of customer accounts and characters with the sole purpose of selling them. Implementation of a random character forces human intervention at the registration stage.

### **Publishing clear disclaimers and risk management requirements.**

Merchants should clearly state on the e-game website that any users or characters found to be utilizing fraudulent payment cards for top-ups will be deleted, and that corresponding account information will be placed on a negative list. Depending on the market, laws and penalties governing e-commerce crimes should also be published prominently on the merchant's website.

## 2. Active Monitoring of the E-game Environment

For e-game merchants, the key to managing fraud risk is the ability to detect characters that have been set up by fraudsters and the prevention of credit top-ups for suspicious characters. Best practice tactics in this area include:

### **Establishing strict criteria(e.g., velocity checks) for character top-ups using payment cards.**

E-game merchants should limit top-ups of game characters for unknown users (i.e., customers not on the positive list). To do this, set a low limit of top-ups for new customer IDs and implement a daily and monthly limit on both the customer ID level and the IP address level. Another criterion that merchants often use allows customers to top up only after a significant amount of "active" game time has been played. This tactic arises from historical trend analysis indicating that fraudulently created characters do not have much "active" game time.

Provide a Customer Call Center. Legitimate customers experiencing difficulties with top-ups can contact your company's Customer Call Center for assistance.

[continued]

<sup>2</sup> The laws relevant to the definition, collection, storage and use of personal information may vary by jurisdiction and should be completed in accordance with applicable law. Card account numbers and other sensitive elements must be handled in accordance with the PCI DSS and, if stored truncated or encrypted.

## 2. Active Monitoring of the E-game Environment [continued]

### Providing top-up verification with both positive and negative lists.

E-game merchants should maintain a positive list of genuine past customers who frequently top up their user accounts with payment cards. To avoid unnecessary service issues with these trusted customers, transactions from these customers should not be routed through risk filters. Similarly, a negative list of customers and the attributes of previously fraudulent transactions should be maintained (i.e., IP addresses, customer names, payment card accounts, cardholder names, and e-mail addresses). Transactions with these negative list attributes should then be declined or flagged for further action by risk management staff.

**Note:** Sensitive cardholder information, such as cardholder number, must be handled in accordance with PCI DSS and, if stored, must be truncated or encrypted.

### Patrolling of the game environment by game administrators.

E-game merchants should monitor the virtual game environment to detect suspicious characters that have been created by fraudsters for reselling purposes. Key criteria used for monitoring includes:

- Suspicious and/or dormant activity in the virtual environment (i.e., characters that generally do not participate in the game properly and are often idle). Game administrators should be wary of characters that possess high value virtual items, but pass or drop them in the gaming world.
- Multiple game characters with the same registration or top-up IP addresses. This usually indicates that fraudsters are creating multiple characters for the purpose of resale.

E-gaming merchants have detected more than 30 characters with a single registration IP address. No customer complaints were received when these characters were cancelled.

## 3. Strong Preventive Measures

In addition to ensuring strict customer registration and actively monitoring the game environment and top-ups, merchants should take strong preventive actions on any detected suspicious and confirmed fraudulent transactions. Best practice tactics in this area include:

### Character killing.

Suspicious characters detected through monitoring by the game administrator or through a positive match with the negative list database at the point of top-up should warrant the consideration of immediate suspension. All other characters with similar attributes (e.g., IP address, e-mail address and/or payment card account numbers) should also be considered for suspension. When implementing *character killing*, merchants should observe market-specific laws regarding consumer protection rights.

### Populating the negative database.

Upon merchant confirmation of fraudulent transactions, e-game merchants should input transaction attributes (e.g., IP address, payment card account number, cardholder name and e-mail addresses) into the “negative list” database. Transactions with these “negative-list” attributes should either be ‘declined’ or flagged for further review by your risk management staff. E-game merchants should also monitor transactions reported by the card issuer as fraudulent (contact your acquiring bank for more information). In addition, incoming fraud related chargebacks should also be included into the “negative list”.

### Shared intelligence.

Where applicable and permitted by applicable law, e-game merchants should proactively share information on fraud patterns and “negative-list” attributes (payment card account numbers may not be shared) with other peer merchants and (or) acquiring financial institutions. This will benefit the e-game industry as a whole as crime syndicates will have greater difficulty attacking other e-game merchants.

For more information, please visit your respective regional website at [www.visa.com](http://www.visa.com).

