



Telecommunication Industry

Global Fraud Prevention and
Best Practices for Visa Merchants



Overview

This document identifies common methods used by fraud rings to exploit the telecommunication industry and provides best practices employed by this industry to combat increasing fraud trends targeting their prepaid mobile cell phone top-up¹ and International Direct Dialing (IDD) account product offerings within their card-not-present (CNP) sales channel.

The CNP Internet and mail/telephone orders sales channel 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 plan 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 telecommunication industry, in particular their online prepaid mobile cell phone top-up and online IDD account product offerings. Typically, the fraud attacks against this industry involve fraudsters offering “discounted” top-up credits on prepaid mobile cell phone accounts or IDD accounts. When cash changes hands, fraudsters or organized crime groups then top-up the credit on a mobile account using fraudulent payment card account details.

The challenge unique to the telecommunication industry is that prepaid mobile cell phone accounts are unregistered, making it difficult to establish customers’ identities.

This document is to be used as a guide for new and existing 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 telecommunication industry.

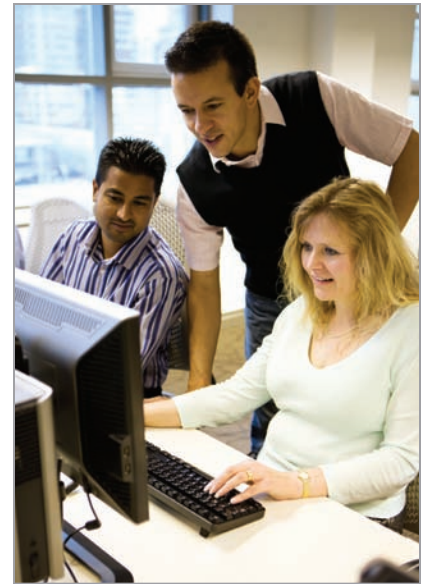
There is no single, simple solution to managing fraud risk. Rather, it is a continuous effort that, involves a comprehensive, layered fraud reduction strategy. This approach combines the use of a variety of risk tools, strategies, and fraud controls that will mitigate incidents of fraud without restricting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

Prepaid CNP Fraud Reduction Best Practices

This best practice guide compiles feedback from telecommunication merchants that have successfully managed online fraud.

In general, online prepaid CNP fraud reduction best practices can be segmented into three continuous parts:

1. Establish strict customer registration policies in which merchants validate users at sign-up;
2. Actively monitor customer accounts to identify suspicious accounts and suspicious credit top-up activities;
3. Take strong, preventive action against identified suspicious characteristics and customers to ensure that these characteristics are not used again in the future.



¹ The term “top-up” represents the purchase of additional airtime using a Visa payment card account.

1. Strict Registration Policies

At the online 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, telephone number, e-mail address and date of birth.² A confirmation code should be sent to the customer's mobile number; the customer's account should only be activated as a result of the customer accessing the account at the portal using this code.

Merchants have determined that restricting accounts to a particular unique mobile number/e-mail address can significantly reduce fraud because this raises the barrier of entry for potential fraudsters.

Each top-up/IDD account must be linked to only one unique mobile number and e-mail address. 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.

Telecommunication 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 card not present 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. Telecommunication 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.

Publishing clear disclaimers and risk management requirements.

Merchants should clearly state on their website that any accounts found to be utilizing fraudulent payment cards for mobile cell phone 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

In addition to increasing and implementing strict user registration policies, merchants should also actively monitor all top-up transactions and mobile/IDD accounts. Best practice tactics in this area include:

Establishing strict criteria (e.g., velocity checks) for mobile cell phone account top-ups using payment cards.

Telecommunication merchants should limit top-ups of phone accounts for unknown users (i.e., customers who are 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's ID/mobile number level and IP address level.

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

Telecommunication merchants should maintain a positive list of genuine past customers who frequently top up their 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 previous fraudulent transactions and fraud related chargebacks should be maintained (e.g., IP addresses, customer names, payment card accounts, cardholder names, mobile numbers 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.

² 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 [continued]

Implementation of real time Fraud Detection System (FDS). A real time FDS would be able to detect high-risk transactions based on previous fraud trends/attributes and flag them for further action by the risk management team. This practice is especially useful for telecommunication merchants with large e-commerce volume because all transactions are monitored on a daily basis. Key risk filters that should be deployed with the FDS include:

- Account number and IP address velocity checks
 - Block IP addresses with a history of previous fraud.
 - Place limits on the value or number of transactions placed from a given IP address (especially non-domestic IP addresses).
 - Block IP addresses with a history of fraudulent transactions or fraud-related chargebacks.
 - Limit the number of payment cards that can be linked to a single IP address within a given time period.
- Prohibit the same card from being used more than “X” number of times, or flag a certain number of transactions made within 24 hours (i.e., conduct velocity checks).
- Prohibit the same card from being used to make payment on more than “X” number of different accounts.
- BIN velocity checks
 - Set strict limits on the maximum value of individual transactions made with non-domestic issued BINs within a given time period.
 - Set strict limits on the maximum value of the sum of all transactions made on a single non-domestic issued BIN within a given time period.
 - Set strict limits on the number of transactions that can be made with a single non-domestic issued BIN within a given time period.
- BIN country and mobile country verification.
- Accounts with excessive usage/call time.
- High ticket value transactions.

Analyze fraud patterns.

Where an FDS is not available, merchants should analyze fraud patterns by isolating high risk IP addresses, payment card account numbers, and mobile cell phone numbers to prohibit use and mitigate incidents of further fraud. This information can then be used to filter incoming transactions where stricter controls are implemented, and may also help limit any reduction in sales volumes of genuine transactions made at the merchant.

3. Strong Preventive Measures

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

Account closure.

Suspicious accounts detected through the FDS or through positive match with the negative list database at point of top-up should warrant the consideration of immediate suspension. An analysis of historical data for all other accounts with similar attributes (i.e., the same IP address or payment card account numbers) should also be conducted; any suspicious accounts detected should also be considered for suspension.

Populating the negative database.

Upon confirmation of fraudulent transactions telecommunication 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. Telecommunication 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, telecommunication 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 telecommunication industry as a whole as crime syndicates will have greater difficulty attacking other telecommunication merchants.

For more information, please visit your respective regional website at www.visa.com.

