ezidebit®
A division of globalpayments

Protecting your business against credit card fraud

July 2018

Contents

Protect your business

Merchants face various risks when accepting credit card transactions. This brochure has been developed to assist you to understand the types of risks you face and actions that should be taken to reduce the risk of loss.

One of the greatest risks to merchants is that of fraudulent transactions.

If you are not careful, fraud can cost your business significant amounts of money. Certain types of merchants - based on type of goods sold - are more prone to fraudulent transactions than others. Merchants should understand their likelihood of being a target of fraud.

It is essential for merchants to have a sound understanding of credit card fraud, how it can be detected and how it can be prevented. These concepts are discussed below for the two broad types of credit card transactions:

- Card Present (face-to-face)
- Card Not Present (including Internet Merchants and Mail Order/Telephone Order (MOTO) merchants)

Note: Under no circumstances should you request that a customer provide credit card details via return email.

Many fraudsters prefer to make Card Not Present purchases due to the anonymity afforded by these payment methods. Card Not Present situations enable fraudsters to place an order over the Internet or via MOTO all over the world. If they reside overseas, the chance of criminal prosecution is much lower, which is an added incentive to this type of fraudulent behavior.

As a merchant you should choose a payment facilitator who has obtained a PCI DSS Level 1 Attestation of Compliance.

Authorisation

It is essential that you understand the term ‘authorisation’ - what it means, and what it does not mean.

What authorisation does mean:

- The card number is valid;
- The card has not been reported lost or stolen (although it may in fact be lost, stolen or compromised (card details improperly obtained or copied) and the card owner unaware);
- There are sufficient funds available to cover the transaction.

What authorisation does not mean;

- An authorisation does NOT confirm the person providing the card number is a legitimate cardholder. The risk remains that the person providing the credit card number has either stolen or improperly obtained the card.
- There is also the risk that the purchaser has compromised (improperly obtained) the card number, without being in possession of that card.

Although it is important to obtain an authorisation for each transaction, it does not protect you from the risk of fraud and chargeback.

Chargebacks

As a merchant, you face the prospect of receiving chargebacks. A chargeback occurs where the cardholder (or their bank) raises a dispute in connection with a transaction made through Ezidebit for your business. Ezidebit will work with you to resolve any disputes, however if a dispute is resolved in favour of the cardholder, the transaction is charged back (debited) to your account. In other words, you lose the full sale proceeds and incur a possible chargeback fee.

Common reason for chargebacks are:

- Cardholder did not make the transaction;
- Cancelled recurring transaction;
- Goods not as described;
- Goods faulty or defective;
- Goods or services not received;
- Failure to respond to voucher requests.

Chargebacks can generally be made by either the cardholder or their bank up to a maximum of 12 months from the date of transaction, or from the date the goods or services should have been provided, where delivery was expected subsequent to payment.

It's important that Card Not Present merchants take steps to identify the purchaser and ensure the transaction is legitimate - this can help reduce the risk of chargebacks. The ways you can do this are discussed in the following sections.

Verification of purchaser

At all times, the onus is on you to verify the purchaser is the genuine cardholder. This applies to all merchants irrespective of the method by which the credit card payments are accepted.

It is particularly important for Internet and MOTO merchants to identify the purchaser; however Ezidebit recommends that merchants accepting credit card payments in a card present environment also take steps to verify the purchaser, especially for large purchases.

If you sell goods to a purchaser who is not the genuine cardholder, you may be liable for a chargeback.

Types of goods fraudsters target

Due to their high value and ability to be re-sold, the following types of goods are frequently targeted by fraudsters:

- Electrical goods;
- Household appliances;
- Jewellery;
- Computers;
- Furniture;
- Goods which are easily disposed of for cash.

If you are selling any of these types of goods, we urge you to be extremely careful before handing over/shipping goods. In particular, take all possible steps to confirm that the purchaser is the genuine cardholder. This applies to all merchants whether selling in a face-to-face or Card Not Present environment.

Detecting suspicious orders

The following are indicators of potentially suspicious Internet and MOTO transactions. Frequently, it is the presence of more than one of these factors that indicates possible fraudulent activity.

- Orders for the types of goods detailed in the 'Types of goods fraudster target' section;
- Unusually large orders;
- Orders of multiple quantities of the same item;
- Customer who place a number of orders within a short space of time;
- Customers who place orders using multiple credit cards;
- Orders placed where the first card offered is declined, and a second card is immediately offered;
- Orders requiring urgent shipping;
- All overseas orders, especially where the order is from a country from which you don't usually receive orders;
- Orders shipped to a country where the goods could easily be purchased locally. The question must be asked why the purchaser is prepared to pay the shipping expense and wait longer for the goods to arrive;
- Orders requesting the goods to be shipped to a post office box;
- Orders requesting the goods to be shipped to a third party;
- Orders made within a short period of time on credit card numbers that are very similar, such as where only the last four digits differ;
- Orders for goods not normally supplied by your business.

While all orders from overseas countries represent an increased fraud risk, transactions originating from the following regions have been identified as generating a disproportionate level of credit card fraud:

- West Africa;
- South East Asia;
- Eastern Europe.

Card Present merchants can also be targeted by fraudsters, however this is less risky than selling in a Card Not Present environment. The indicators below are useful to detect potentially suspicious purchases:

- Orders for types of goods detailed in the 'Types of goods fraudsters target' section;
- Unusually large orders;
- Customer who purchases multiple numbers of the same item without regard to size, colour, style or price. Merchants should ask themselves whether it is likely that an individual would purchase a large number of a particular item;
- Customer who don't negotiate on price where it is customary to do so. The possibility exists that the person isn't concerned about the price because they have no intention of actually paying;
- Customer purchasing large and bulky items, but refusing home delivery despite its inclusion in the price. It may be that the customer doesn't want the merchant to know their address due to the purchase being fraudulent;
- Customer offering more than one credit card in connection with a single purchase;
- Customer who makes repeated purchases in a short period of time;
- Customer who pulls their credit card out of a pocket rather than a wallet;
- Customer who appears anxious, nervous or impatient;
- Customer who tries to distract you at the time of processing the transaction, especially where the transaction is large;
- Where a large purchase is made on a newly valid card. The reason is that credit cards are sometimes stolen while being sent from the bank to the rightful cardholder.

Protecting your business against fraud

Apart from being alert to potentially suspicious transactions, a merchant's main defences against fraud in card present situations are to carefully inspect the card to ensure it is genuine, insert the card when prompted by the payment terminal, authenticate the transaction using a PIN as prompted by the payment terminal, and where applicable check that the signature on the back of the card matches the purchaser's signature on the sales voucher.

The payment terminal will prompt for authentication by PIN, or authentication by signature or note that authentication is not required, depending upon the nature of the transaction. Merchants should follow terminal prompts at all times and refrain from hand keying transactions for any reason when the card and purchaser are present, particularly where this is suggested by the purchaser. Hand keyed transactions shift liability to the merchant in respect of fraud chargeback reason codes because this practice circumvents security and authentication features on the card and the terminal.

The following security checks should also be performed:

- Closely inspect the card. Check that the 'valid from' and 'valid through' dates include the current date;
- Check the card has the appropriate security measures;
- Check the first four digits of the embossed account number match the four digits printed immediately above or below the embossed number;
- When tilting the card, the hologram on Visa and Mastercard credit cards should move and/or change colour;
- On the signature panel on the back of the card, check that the words 'Visa' and 'Mastercard' appear repeatedly at a 45 degree angle;
- Check that the abbreviated credit card number on the sales receipt matches the corresponding digits on the card. If the digits don't match, this is a clear indication the card is counterfeit;
- Closely inspect both the front and back of the card to determine whether any part of the card appears to have been altered.

Protect your business against Internet and MOTO fraud

Merchants can minimise the possibility of fraudulent purchases and chargeback from Internet and MOTO transactions by implementing the following measures:

- Request the name of the cardholder's bank. Fraudsters who have compromised account details will not have this information. If the purchaser hesitates in advising the name of their bank, caution should be exercised;
- Request the purchaser to provide an email copy of their driver's licence;
- Ensure the customer's billing address and delivery address are consistent;
- Never forward goods to a post office box;
- Obtain a signed receipt from the cardholder when goods are delivered;
- In the case of orders for a large number of different goods, telephone the cardholder after the order is placed to confirm the order. Also, have the purchaser read back all details of the order. Frequently, where an order is fraudulent, the purchaser will be unable to confirm those details, as they were ordering at random, with no record of what they ordered;
- Be suspicious where multiple cards are used for a single purchase;
- Don't continue to attempt authorisation after receiving a decline;
- Exercise particular caution in relation to overseas orders. Large orders should in all cases be held back for shipping while the above enquiries are made into the legitimacy of the purchaser. Merchants should not ship goods until satisfied that the purchase is legitimate.

TIP: Never process a refund transaction to a different card, in cash, by cheque or by electronic money transfer.

Protecting yourself from funds transfer fraud

What is it?

Funds transfer fraud continues to be a widespread issue for merchants. It involves the use of stolen credit card information and seeks to obtain funds by money transfers.

How does it work?

The ultimate goal of the scam is to trick you into providing funds to the fraudsters or an unfamiliar third party (who is often working for or has been set up by fraudsters) through another form of payment, such as a different credit card, cash, cheque or other form of electronic money transfer. This alternative form of payment may take the form of a refund or request to organise shipping with a specific courier that doesn't actually exist.

Example

In this context, fraudulent cards are used to purchase goods/services, and then the (supposed) cardholder requests a component of the card transaction value to be paid to an associated third party. For example, $4,000 of car parts are purchased via a telephone order and the cardholder asks the merchant to cover the $1,000 cost for the courier services by money order, taking the total transaction value to $5,000. The merchant pays the courier $1,000 by money/bank transfer, which becomes a straight loss. The rightful cardholder then claims the transaction is invalid (or disputes liability) and the transaction is reversed, and $5,000 is charged back to the merchant's account once the dispute has been completed in favour of the legitimate cardholder. The merchant will incur additional loss if the goods were exchanged.

What should I do?

- Use your instincts - if the sale seems too good to be true it often is;
- Only process refunds to the credit card used in the original transaction;
- Refrain from sending funds by electronic funds transfer in this context;
- Review transactions that carry an increased fraud risk, including overseas orders from West Africa and Eastern Europe;
- Be wary of 'hard luck scenarios'. Often these scams seek to take advantage of your goodwill.

Sales refunds should only be processed to a card where there was an initial valid transaction on that card. A sales refund must not be provided to a different card, in cash or by cheque.

Other risks merchants face

Fraudulent refund transactions

A common type of fraud involves employees issuing credits (refunds) to their own account. To avoid detection, they may create a large debit transaction on a fraudulent card and an offsetting credit on the own card. In this type of situation, it is likely to take weeks, even months, before the fraud is detected. To guard against this type of fraud, we recommend that merchants closely monitor all credits, and check that all credits and corresponding debits relate to the same card number. Particular attention should be paid to large credits.

Another way in which merchants can protect themselves from this type of fraud is by regularly changing their terminal or user password(s), especially after an employee has left.

Online authentication of purchases

The primary risk facing merchants accepting Internet transactions is the difficulty faced confirming the purchaser is the genuine cardholder. Where a cardholder disputes having made an online purchase, irrespective of whether this is actually the case, the merchant is generally liable for the chargeback.

Visa and Mastercard have jointly attempted to overcome this burden placed on Internet merchants by developing an online cardholder authentication service known as 'Verified by Visa' and 'Mastercard SecureCode'. A term called '3D Secure' refers to the technology platform though which this service is offered.

The primary benefit to merchants of these verification processes is the chargeback liability shift that occurs. Subject to a few exception, if a merchant attempts to authenticate a purchaser using 3D Secure, both the cardholder and their bank lose the right to make a chargeback claiming the cardholder did not make the transaction. This is irrespective of whether the cardholder or their bank subscribes to 3D secure - all that matters is that the merchant has implemented 3D secure, and attempted to verify the cardholder's password.

Of course, if the password verification check fails (the purchaser entered the wrong password), you should not proceed with the transaction. If you proceed with the transaction after a cardholder has failed the verification check, you will incur the liability should a chargeback result.

For further information on how to protect your business from fraud please contact support@ezidebit.com.au

For Further Information

Call: 1300 763 256
Visit: www.ezidebit.com
Email: support@ezidebit.com.au

ACN 096 902 813
AFS License 315388