globalpayments

Fighting Fraud At Every Level

Fraud is an ever present drain on your profitability. While it may be a relatively small percentage of your total revenue, just think what else you could have used that money for. But more worrying is the fact that any single fraud could be for ***any*** amount of money – and if it's affected one of your customers, they could consider you to blame.

As one of our customers, you're already well ahead of the game. It means you've chosen a card payment provider who's consistently at the forefront of fraud reduction. The awards we have received, such as The Best Security or Anti-Fraud Development Award at the Card and Payments Awards 2011 and the Merchant Award at the 2011 ECAF Awards aren't just congratulatory badges; they are a demonstration that we lead the field in protecting you and your customers from the distress and expense of card fraud.

Understanding Card Fraud

The best anti-fraud measures are the ones that prevent the crime happening. You need to be vigilant and you need to understand how some of the more common frauds are perpetrated. So come with us now on a brief tour of the fraudster's world.

Face-to-Face (Customer Present) Transactions

First we'll deal with a few fraudulent goings on when the customer's there in person. Bear in mind that the criminal could be the customer or even your own member of staff – and sometimes both.

Non Chip and PIN Payments

Chip and PIN cards have vastly improved the security of card payments. Unfortunately, they're not as widespread as you might think. The UK was the first major country to switch completely to this system; most other countries still use the less secure magnetic stripe and signature method. Until these other countries upgrade their processes, you may still be required to accept payment on signature.

While you can't discriminate against non-PIN customers, you can certainly be more vigilant if a customer presents a card which requires a signature or claims that the chip on their card has been damaged. Watch how the customer signs the slip: does he or she appear to be copying their "own" signature from the back of the card? Does the flow of the pen appear natural? Do the signatures actually match?

Also be alert for transactions with an obvious benefit for the fraudster, such as cashback.

Skimming Devices

A skimming device intercepts card data – often including the PIN number – before passing it on to allow the payment to continue normally. The devices can simply be small hand-held scanners concealed in a pocket, or sophisticated appliances like keypad overlays that record keystrokes. You should inspect your payment terminals and ATM machines regularly and carefully. The devices can be quite hard to spot, look closely for tell-tale signs like a raised lip around the keypad or an unfamiliar rim on the card slot.

Mobile Phones

One trick used by unscrupulous checkout staff has been to carry out a pretend telephone conversation while handling a customer's payment. In fact they were actually using their phone to video the customer's PIN, card number and even their security code from the back of the card.

Customer Not Present Transactions

The scams we've covered above require the physical presence of the customer and the fraudster (who might be the same person). However, more and more transactions take place where the customer and the merchant never meet. And this can increase the opportunity for fraud.

These are the most common types of customer-not-present (CNP) transactions:

- Mail order.
- Telephone order.
- Faxed order.
- Internet order.
- Recurring transactions

There are many potential compromises to payment security here: telephone conversations can be overheard; faxed orders can be left lying in the machine's tray; websites can be hacked. As a result, any disputed transaction will ***often*** result in a chargeback on your account.

Protecting Card Information

Part of the defence against CNP fraud is to make it more difficult for the scammers to obtain usable card information. You'll notice that your card receipts no longer carry your full card number; instead you'll see "XXXXXXXXXX8006" or something similar. It's enough information to remind you which card you used, but not enough to be of use for the criminal. We were one of the first companies to introduce this security, though it's now in place everywhere in the UK.

The card security code – or AVS/CV2 number – is the three digit number from the back of the card that you usually provide when you make a CNP payment. This code is intended to verify that the purchaser is actually in possession of the card. But problems occur when the code is stored insecurely. Our recommendation here is not to store it at all, but bear in mind that simply deleting data from a computer is not enough!

Internet Transactions

Word Wide Web card transactions should always be carried out using a Secure Socket Layer (SSL). This usually means that the Web address will begin with "HTTPS". SSL encrypts the information that your customer exchanges with the payment system, protecting it against interception by hackers. We require a minimum of 40 bit encryption, though most SSL implementations nowadays use our preferred standard of 128.

It's a common misconception that SSL refers to a secure server. If you store card information on your own server, it's important to understand that SSL refers only to the method by which information passes between your server and your customer – it does **not** secure the data on the server itself. This means that you need to ensure that this information is stored securely, ideally in an encrypted form.

Both MasterCard and Visa have introduced additional security procedures for Internet transactions. Both MasterCard SecureCode and Verified by Visa provide an extra layer of protection, known as 3DSecure. You can easily offer these schemes by using our Global Iris payment service, or we can guide you through setting up your own access to them if you prefer. It's well worth implementing 3DSecure in your transaction process as it protects you from the majority of CNP chargebacks arising from disputes.

What We're Doing

We're constantly working on your side to detect and prevent fraud. We monitor unusual behaviour on an account, untrusted payment sources, suspect IP addresses, and we collaborate widely with international

bodies to detect emerging patterns and trends. It's a constantly changing world, but we're committed to staying at the forefront of fraud detection and prevention.

What You Can Do

Be alert, be conscientious, and stick with best practice. Watch out for tell-tale signs that something isn't right, for example:

- Goods to be delivered to a temporary address like a hotel, or collected by courier
- Purchases where the delivery address differs from the card address (under the distance selling regulations, you should deliver only to the cardholder's address)
- Awkward or unusual behaviour from staff or customers
- Unexpectedly high value transactions

Most of all, ask for advice. We'll always try to help you to stay clear and blame free and our experienced anti-fraud team are on hand to answer any questions that you may have.