Bulletin 40
December 2003

Online and Offline Credit Card Fraud: hazards for small business

In this issue: a discussion of the issues arising for small business merchants accepting credit card payments for online, mail, telephone and face to face sales.

Introduction

Although the focus of this Bulletin is on Internet sales, similar issues can arise not only with other transactions where the purchaser is not present, such as those over the telephone, but also with face to face transactions.

The Internet is a valuable tool for business. It can enhance access to potential customers and new markets, provide the opportunity for efficient dissemination of product information and contract documents and allow new or niche businesses to establish a presence at relatively low cost. The basic principles of good business, however, still operate in the online environment and success or failure will depend on long established factors: living up to your promises, generating business through customer to customer recommendation, good record keeping and credit management systems and being alert to the possibility of fraud.

Security and fraud have always been issues for business, and credit card fraud is clearly an issue for businesses not transacting on the Internet. The speed and reach of the Internet, however, and the possibilities for theft of credit card details have meant increased risk for a business accepting payment with a stolen credit card for an online sale. The consequence will usually be that the transaction is charged back to the merchant – the previous credit to the merchant and debit to the cardholder will be reversed. This will in most cases take place after the goods have been dispatched, resulting in loss to the merchant.

Increase in disputes

This office has seen a recent increase in disputes brought by small business bank customers about charge backs of credit card payments arising from online sales. In most cases, the businesses took some precautions but either did not understand the limitations of information from their bank about whether the transaction was authorised or did not recognise warning signs that indicated potential fraud.

OMBUDSMAN

BULLETIN

Banking and Financial Services Ombudsman Limited

GPO Box 3A,
Melbourne 3001.
DX 221 MELBOURNE

Telephone: 1300 78 08 08
Facsimile: (03) 9613 7345

www.bfso.org.au

A.B.N. 48 050 070 034

The purpose of this Bulletin is to make some observations about the patterns in credit card fraud in the cases that we are seeing, using case studies as illustrations. The observations and case studies should be kept in perspective. An Internet presence can provide competitive advantage and growth to a business. We see transactions that go wrong, not the millions that occur without mishap.

The Bulletin also raises some currently unresolved issues about card scheme databases of businesses that have had their merchant facility terminated and the broader issue of contractual allocation of risk.

We hope that this Bulletin will be helpful for small businesses and small business associations, in conjunction with a number of other initiatives and resources described at the end of the Bulletin. It is important that small business owners are aware of the risks so that they can be weighed against the benefits offered by online and other credit card sales. It is also important that they educate themselves about and implement risk reduction strategies.

'Authorisation' of the transaction by the bank does not mean authentication of the customer. Under the contract, the merchant bears the risk that the customer is not the true cardholder.

It is a common requirement for businesses with credit card merchant facilities to seek authorisation from the bank for a transaction above a certain monetary limit. The merchant rings the specified number or uses the terminal, provides the credit card details and transaction amount and, unless the transaction is declined, receives an authorisation number. In the cases we see there is a common misunderstanding on the part of merchants that this amounts to verification that the transaction is genuine. In practice, such authorisation means only that the card number is a valid card number and that there are sufficient funds in the account. Such authorisation does not prevent the transaction being charged back if the credit card details were stolen and the true cardholder disputes the transaction. Our view is that the word 'authorisation' should be replaced by another word that does not confuse it with cardholder authorisation of the transaction.

Misunderstandings may be aggravated if the merchant seeks reassurance from the bank about whether a transaction is genuine or 'safe' to proceed with. We see cases of apparent miscommunication between the bank and the business customer where the information provided by the bank in response to such a request is interpreted by the customer as an assurance that there is no risk in proceeding with the transaction. This office will take into account the communication between the financial institution and the merchant to determine if there has been a misrepresentation about the risks.

The merchant agreement between the bank and the business and the Operating Guide and other information provided to the business are usually clear in warning that authorisation for a transaction does not guarantee that the purchase is being made by the cardholder. They also, usually, clearly state that the transaction may be charged back if it is disputed by the true cardholder. Unless it is established that the merchant received and relied upon misleading advice or information from the bank, this office will, usually, allocate liability to the merchant in accordance with the merchant agreement. Although misleading advice will be difficult to establish where there is a direct conflict in the recollections of the merchant and the bank officer concerned in the absence of records of conversations, there have been cases where this office has been satisfied that the explanation given has been misleading.

It is important that bank staff who are asked for reassurance about a transaction by a merchant state clearly that:

- authorisation of the transaction does not mean that the true cardholder has authorised the transaction;
- authorisation does not protect the merchant from charge back; and
- the bank cannot guarantee that the transaction is being conducted by the true cardholder.

This information is usually in the merchant agreement or the facility Operating Guide but it should be repeated in response to a telephone or in-branch inquiry to reduce the possibility of misunderstanding on the part of the merchant, and because more attention is usually paid to what is said than what is written. It should also, ideally, be explained at the time of installation, and the explanation acknowledged in writing by the merchant.

Be aware that the transaction may be charged back several months after you sent the goods

A fraudulent transaction may not be discovered by the true cardholder for some months depending on when in the statement cycle it was processed. The fact that the transaction has been authorised and the merchant's account credited with the funds does not mean that the payment is 'clear'. This creates a dilemma for merchants as they will usually have an obligation under the merchant agreement with the bank to supply the goods or services before processing the credit card transaction, in addition to their obligations under the contract with the customer.

Fraudulent purchases put more than the purchase price at risk: termination of the facility and listing

Being targeted by fraudsters, whether online, over the phone or in person, may result not only in charge backs but also in the termination of the merchant facility and the listing of the business on credit card scheme 'terminated merchant facility' databases.

In a number of recent cases the dispute has been about the fact that, as well as charging back disputed transactions arising out of apparently stolen credit card details, the bank had exercised a contractual right to terminate the facility and had also 'listed' the merchant with databases held by the credit card schemes and accessible by other participating credit providers. In some cases the existence of the listing had been given to the merchant by another bank as the reason why they had declined to grant a replacement facility.

The contractual right to terminate the facility appears likely to be exercised when the merchant:

- has a high 'fraud to sales' ratio;
- is apparently being targeted by fraudsters;
- has shown a failure to take reasonable care; or
- is suspected of being involved in the fraud.

In each case the bank stated that it was obliged to list the merchant as one that had had its merchant facility terminated under its contracts with the credit card schemes and to use one of a number of specified reason codes. The disputants say that they did not know that this would happen, that the listing reasons used implied involvement with fraud, even though the merchant had been the innocent victim, and that the listing had made it difficult to obtain another merchant facility.

The cases raise a number of issues:

- Is there a contractual right to list?
- Is the listing process adequately disclosed to merchants?
- What is the potential loss?
- Does a merchant in such a case have a claim for injury to reputation where they are targeted by fraudsters but not involved in the fraud?

Injury to business reputation is, in accordance with our Guidelines, an issue more appropriately dealt with by a court because of the need for evidence from third parties. The issue of immediate concern to this office is whether the listing process is adequately disclosed. This is an issue that requires further consideration and discussion and we welcome feedback on the legal and policy issues involved.

There is no doubt that credit providers should have the right to terminate merchant facilities on reasonable grounds or on adequate notice. It is clearly arguable that other merchant facility providers have a legitimate interest in knowing whether and for what reason a merchant applying for a facility has had a previous facility terminated. Given the importance of access to the credit card payment system for businesses and the apparent detriment caused by listing for reasons using the 'fraud' reason codes, however, merchants should know about the process. Knowledge that being the target of fraud could lead to such a listing would underline, in our view, the importance of taking care in the acceptance of payment and not ignoring doubts about the identity of the purchaser or the genuineness of the purchase.

Our preliminary view is that the merchant agreement should clearly state that the merchant is authorising the bank to provide information concerning the termination and the reason for the termination of the merchant agreement to the card schemes for use by participating merchant facility providers.

Case Study 1

This dispute related to charge backs on A's company account. The transactions originated from email orders received from Indonesia from people who had apparently visited A's web site and who were associates or friends of the person who made the initial enquiry. The purchasers used stolen details of US cards.

There were a number of unusual features about the orders:

- *Although A's business was gym equipment, the apparent purchasers also asked if A could source mobile phones;*
- *When one card number was declined it was suggested by the purchaser that another card 'in his wife's name' be tried;*
- *The initial purchaser was prepared to pay a 'premium' for the phones but asked that the customs declaration not state that mobile phones were included in the package;*
- *The language of the emails suggested that English was not the purchasers' first language in contrast to the Anglo names under which they communicated and which were given as the cardholders' names.*

A said that he had relied on assurances from bank branch staff that it would be safe to ship the goods if authorisation was received. There was a dispute, however, about what exactly had been said. A said that he asked for re-assurance that, provided he had gone through the correct procedures, if the transactions were approved that would be the end of the matter so far as the bank was concerned. He told this office he understood that if the customer disputed it he would be liable but because the people he was dealing with seemed satisfied and he had no reason to believe they were other than the cardholders, he thought there would be no problem.

Some common threads

We have observed some patterns in the cases considered by this office where the purchaser is not the true cardholder and charge backs have resulted:

- The customer offers numerous credit cards and may ask for them to be tried in succession or the transaction split across them;
- If the first amount is declined the customer asks that the amount be reduced until the transaction is authorised;
- The customer requests goods other than those usually supplied by the business;
- The customer follows up a small initial order with large and multiple orders;
- The customer may ask that the shipping or customs documents not disclose the goods in fact being shipped or that the value be understated;
- The customer requests goods without apparent concern as to price but with a clear concern for speed of delivery.

This is not to say, of course, that these factors will always indicate fraud. Some people do hold numerous credit cards and if one is declined offer another. But they are common threads in the cases we see where the purchaser is otherwise unknown to the merchant, is not physically present and is not the true cardholder.

Things to remember:

- Read and be familiar with your merchant agreement, merchant operating guides and all other documentation governing the use of the facility. Make sure all staff using the facility are familiar with these;
- The fact that funds are credited to your account does not stop the transaction being later charged back. Authorisation and credit of funds do not guarantee that the transaction is genuine;
- Be wary of anyone who offers numerous credit card numbers;

The bank stated that the question asked was whether it would be ok if you get authorisation for a credit card transaction. The bank officer concerned said that she replied it should be ok but when the disputant mentioned orders for phones from overseas she made a reference to recent publicity about stolen cards.

The case manager's view was that, even if the conversation was as recounted by the disputant, in seeking advice the disputant had not provided sufficient information about the nature of the transactions to enable the bank to give informed advice, nor was it reasonable to conclude from what had been said that authorisation made the dealings with the intended customers safe. The information known to the disputant but not to the bank raised or should have raised a reasonable suspicion of fraud and the case manager found that the disputant had failed to exercise reasonable care, as required under the merchant agreement.

Case Study 2

B's company operated an Internet based business retailing DVDs and videos and were authorised to accept mail and other credit card sales. In August 2002 they applied for and the bank agreed to provide them with a security gateway that kept the customer's credit card details secure. B understood that authorisation via this gateway would also provide protection against fraud for the business but in fact, as the Letter of Offer for the gateway and other contract documents made clear, authorisation via the gateway does not guarantee that the purchase is being made by the cardholder and charge backs can still occur.

In early March 2003, B accepted and fulfilled a sales order from Russia after the bank had confirmed payment approval via the gateway.

- Do not accept 'authorisation' to debit a card from a person claiming to be the wife, husband, partner, friend etc of the cardholder. Only the actual cardholder can authorise a payment;

- Be wary of any person who asks you to sell them goods that you do not usually deal in or asks you to provide cash in return for a debit to a credit card. Apart from charge backs, you run the risk of being in breach of your merchant agreement;

- Do not allow your merchant facility to be used by anyone other than you or your employees;

- Be wary of a single order from overseas followed by large and repeated orders from friends or associates of the original purchaser;

- Take additional steps to check that the customer is the cardholder. These are likely to reduce, but will not eliminate, the risk of a charge back.

Resources for small business

There is no doubt that government and industry recognise that fraud is an issue hampering the use of the Internet to its full economic potential and causing loss to business and consumers. Work is being done not only to improve security, including security of payment, but also to educate business and consumers about the risk of fraud and risk minimisation strategies.

As a first step it is important that business owners read their merchant agreements and the information provided to them by their bank carefully, particularly alerts or bulletins to do with fraud and security. This appears to be commonly overlooked, often for purely human reasons of time constraints and, possibly, a sense that 'all we need to know is how to operate the machine'. It is, however, important information, not the least because the contract documents make it clear that the risk of fraud is allocated under the contract to the merchant.

One member bank, in conjunction with a major credit card issuer and a specialist risk reduction advisory firm, has over the past few months been travelling around Australia inviting retail merchants to Credit Card Fraud Prevention seminars. The seminars provide a brief background into the operations of

That sale appeared to result in numerous other orders from customers in Russia. Between March and May substantial new business was generated. In late April the bank advised B that the sales transactions to Russia had been charged back and appeared to be fraudulent. The charge backs overdrew B's business account by $12,000. Two months later the bank served demand for immediate payment of the overdrawn amount. B said that the business was unable to sustain the loss and had ceased trading.

B claimed that the business loss could have been avoided had the bank provided them with sufficient information about the high degree of exposure to fraudulent transactions over the Internet and the allocation of risk and liability, together with fraud minimisation information.

They acknowledged that information about these matters was in the merchant agreement and operating guide provided to them but said that they had relied on the conversation that they had with the bank's business payment consultant who, they said, had failed to warn them of the risks.

The bank's records indicated that this additional warning was recommended but the case manager was not satisfied that it had been given. Although there was no misrepresentation as such and the contract documents were clear, because good banking practice and recommended internal procedures had not been followed, the Finding was that the bank should not recover interest and fees on the overdrawn balance of the account and should enter into a repayment agreement for repayment of the principal debt.

major crime syndicates and how they target merchants with stolen or counterfeit credit cards. Fraud indicators and risk reduction strategies are discussed. Such initiatives, and merchant participation in them, are to be encouraged.

The National Office of the Information Economy has useful information on its web-site www.noie.gov.au, including a package of information on e-business security for small to medium enterprises, 'Trusting the Internet'.

As always we welcome feedback about the issues raised in the Bulletin.

The Banking and Financial Services Ombudsman wishes you a safe and happy Christmas and holiday period

Case Study 3

C's company manufactured and exported exercise equipment. In 2002 it began selling to retail customers via its web site, including to overseas customers. In November and December 2002, it received orders from Indonesia for equipment to the value of $20,000 with a request to split the price of the goods over eight credit cards. C received authorisation for the transactions and shipped the goods.

In January 2003, it received orders from a different individual from Indonesia but again with a request to split the full price of the order over six credit cards. When authorisation was sought it was declined. In a conversation with a bank officer about the implications of the decision to decline, C's manager was told that there was a risk that the previous orders may be fraudulent. The transactions were in fact disputed by the true cardholders in late January 2003 and charged back to the merchant – all the cards were issued by a US bank to US citizens.

C's dispute was that it had relied upon what it regarded as the bank's approval of the November/December transactions to send the goods. The merchant agreement, however, clearly stated that a transaction was invalid and could be charged back if it was not authorised by the cardholder. The Merchant Operating Guide provided to the business also made it clear that the purchaser's bona fide's were accepted by the merchant at its own risk and that when authorisation is obtained it does not guarantee that the purchase is being made by the cardholder.

This office's view was that in the circumstances there had been no misrepresentation and no other reason to allocate liability other than as under the contract.