BFSO Bulletin 43
September 2004

In this issue:

- Credit card and electronic payment systems – issues for financial services providers.

  A discussion of issues for financial services providers arising from the use of credit card and electronic payment systems by small business merchants.

- Proportionate Liability for Misleading Conduct

- New Chairman of the Board of BFSO Ltd

OMBUDSMAN

BULLETIN

Banking and
Financial Services
Ombudsman Limited
GPO Box 3
Melbourne 3001
Tel: 1300 78 08 08
Fax: (03)9613 7345

www.bfso.org.au

A.B.N. 48 050 070 034

Small business merchants' use of credit card and electronic payment systems – issues for financial services providers

For some time now, BFSO has been considering disputes between member financial services providers and their merchants. In Bulletin 40 (December 2003) we discussed some of the issues arising for small business merchants accepting credit card payments for on-line and off-line transactions by mail, telephone, internet and face-to-face. The Bulletin contained some tips for minimising the risks associated with credit card transactions.

In this Bulletin, we again discuss issues affecting small business merchants using credit card and electronic payment systems but this time with a focus on issues facing financial services providers. We hope that by sharing the knowledge gained when investigating these types of disputes, we can promote best practice and reduce the number of disputes coming to BFSO.

Types of disputes

BFSO deals with disputes from small business merchants about:

- the information provided when the merchant facility was installed;
- the information provided when the merchant called the merchant help line;
- the rights and obligations of the parties when there are chargebacks;
- the rights and obligations when the merchant agreement is terminated; and
- the right to list the termination of a merchant agreement on a credit card scheme data base.

Training

Merchants who bring disputes to this office about their merchant facility very often raise a question about the amount and quality of the training they receive in relation to the use of the merchant facility. It is common for merchants to say that the terminal was delivered and that no training was provided at all, or that only very basic training was provided.

From our experience, disputes could be reduced by a clear explanation about how the facility is to be used and the limitations on the use of the facility, for example, whether there is authority to use the facility for mail, telephone and internet transactions. The training could also cover the risks of processing transactions "off line" and conduct or transactions that constitute a breach of the merchant agreement. For example, the training material could make specific reference to splitting transactions, that the facility should only be used for a business purpose and not to conduct transactions for family and friends and how to reduce the risk of fraudulent transactions. Consideration should also be given to the provision of training in a language other than English for merchants whose first language is not English.

Both merchants and the financial services providers would benefit from a more formalised training regime and the documentation of what information was provided. Such training is likely to reduce the incidence of misuse of merchant facilities and reduce the risk of loss due to fraud.

We are aware that on-line training has been developed for various internal bank training programs relating to FSR and Code of Banking Practice compliance and it appears that on-line training for merchants and their staff about the use of merchant facilities would have the following advantages:

- Current issues, such as fraud alerts, can be highlighted in the training;

- The training can be conducted at a time more suitable for a small business owner. For example, rather than leaving the business to attend a seminar conducted by the bank, the merchant can complete the training after hours;

- Given staff turnover may be an issue for some small businesses, it can be incorporated into the induction process for new staff;

- On-line training can be centrally assessed by the bank and records readily retained of the fact that the merchant has undergone and completed such training. If necessary, those records can then be forwarded to the BFSO in the context of a dispute; and

- While videos, bulletins and warnings on monthly statements are useful in highlighting issues to merchants, they are not always viewed or read by merchants (even if they should be.) On-line training provides an opportunity to bring home the current issues in a more targeted and direct manner.

If on-line training is not considered an option for all merchants, best practice could involve the provision of on-line training for merchants in high risk industries or where the merchant is considered to be of a higher risk.

Where training is provided by installers or other agents of the financial services provider, checklists ought to be developed to show that relevant areas of training have been provided and those checklists ought to be signed by the merchant and retained by the financial institution, so that records of such training can be provided to the BFSO in appropriate cases.

Meaning of "authorisation"

In many cases we consider, merchants call the help line for assistance to process transactions or for reassurance about the validity of the transaction. It is clear that there is often confusion in the minds of merchants about the meaning of "authorisation" and that the confusion is not diminished in some cases, after a call to the help line.

Many merchants believe that when a transaction is authorised, either over the telephone or via their terminal, that the cardholder has authorised the transaction. In fact, all authorisation means in this context, is that the card being used in the transaction has available credit and has not been reported lost and stolen. It does not mean that the cardholder has participated in the transaction and therefore "authorisation" does not confer any guarantee that the transaction will not be disputed later by the true cardholder.

This limited meaning of "authorised" is potentially misleading and it is preferable that a more accurate term is used when processing credit card transactions. Our view is that credit card schemes should be encouraged to replace the word "authorisation" with another word that does not confuse it with cardholder authorisation of a transaction.

Improved record keeping

Disputes could be reduced by better record keeping on the part of both merchants and financial institutions. Merchants must be made aware of the need to retain transaction records for the relevant time and of the need to produce records within specific time limits if there is a chargeback request by the cardholder's financial institution.

In addition to keeping records of the training provided, whether in person or on-line, best practice would dictate that financial services providers retain records of the communication between them and the merchant throughout the period that the merchant facility is provided. It is disappointing to note in some cases we have considered that the financial services provider has not retained a copy of the signed merchant agreement and records of significant changes to the terms of the merchant agreement, such as a change in the merchant's floor limit.

It is also quite common in disputes, that there are differing recollections of what was said between the merchant and the operator on the help line. What was said and the information exchanged between the bank and the merchant is often critical to determining the merit of a claim but in many cases, there are no records of the conversation held by the financial institution.

It would not only assist the investigation of disputes, but would also assist internal quality assurance of the telephone operators, if financial institutions developed systems to record the substance of a conversation with a merchant on an electronic database.

Review of merchant agreements

Merchant agreements should be in plain English. Most merchant agreements we have considered fully disclose what constitutes prohibited use of the merchant facility and therefore what conduct or type of transaction will be in breach of the merchant agreement. Termination of the merchant agreement and withdrawal of the facility can be a consequence of a breach of the merchant agreement. Disputes about terminations of a merchant facility are likely to be reduced by the implementation of the enhanced training procedures and record keeping discussed earlier.

Termination of the merchant agreement

However, where despite such training, it is still necessary for the financial services provider to consider terminating the merchant facility, then the financial services provider must ensure that:

1. There are grounds under the terms of the merchant agreement for termination; and

2. The procedure for termination is in accordance with the merchant agreement and is fair in all of the circumstances.

In some cases we have seen, merchant facilities have been terminated because of an excessive number of chargebacks or because of a higher than acceptable chargeback to sales ratio over a certain trading period. These specific reasons for terminating a facility are not usually described in the merchant agreement. In the absence of such disclosure care must be taken to ensure that there are other grounds to terminate the agreement. This is particularly important in cases where the merchant claims to be a victim of fraud by their 'customer'.

In this regard, financial services providers should, in our view, be reluctant to rely on a provision that the agreement can be terminated without notice and without providing a reason. Such a provision may be construed in relevant cases as an unfair contract term under the Victorian *Fair Trading Act*, if the merchant is Victorian based. It may also be "unconscionable" when one has regard to the factors set out in section 12CC of the *ASIC Act*.

Summary – Termination of Merchant Agreement

Before terminating a merchant facility, in our view, members acting diligently and prudently ought to consider the following matters.

It may be appropriate to issue a warning rather than terminate the facility if:

- The member has not done all it can to ensure that the merchant and its employees have been properly trained in relation to the use of the facility, or if the member has not retained adequate records of the training;

- The merchant has acted in accordance with that training and any other information provided by the bank;

- There has been a course of conduct established over a period of time which could be construed as an estoppel, so that the member is prevented from departing from that course of conduct without providing reasonable notice. For example, where MOTO transactions have been allowed in breach of the merchant agreement for a number of years before disputed transactions alert the financial services provider to the operation of the merchant facility by the merchant; or

- The relationship manager or the merchant's branch have made a statement about how the merchant facility can be used in particular cases.

Other considerations may include:

- Is immediate notice of termination justified in the circumstances or should the member give a longer period of notice as specified in the agreement, for example 30 days?

- Has an event of default arisen, having regard to the terms of the merchant agreement?

- Is the event of default of sufficient seriousness that termination is appropriate?

- Does the termination notice accurately reflect the terms of the merchant agreement? and

- Has the notice been served in accordance with the terms of the merchant agreement, for example, is written notice rather than verbal notice required?

Once the agreement has been terminated, it is important for the financial services provider to retain a copy of the termination notice and the details recording the service of that notice, so that it can be produced to the BFSO should there be an issue about the actual circumstances of termination.

Listing termination on a credit card scheme data base

Where it is intended that the fact of termination is to be listed with a credit card scheme, then the provisions in the merchant agreement relating to listing ought to clearly disclose the possibility of listing and provide a contractual authorisation for the disclosure of such information, having regard to a bank's implied duty of confidentiality and the provisions of the Privacy Act, if applicable.

BFSO is of the view that given the serious consequences that can flow as a result of being listed with a credit card scheme as a terminated merchant, the merchant's attention should be drawn to this provision in the merchant agreement. There may be benefits to the financial institution if this clause were emphasised because knowledge of the consequences of listing may act as a deterrent to misuse of the merchant facility.

Case Study – Termination of Merchant Facility

The Dispute

Mr A 's business provided an on-line form guide for horse racing. The merchant agreement gave Mr A approval to accept Mail Order, Telephone Order and Internet Order sales. In order to offer additional security to the business' subscribers, Mr A utilised the services of a gateway that protected the cardholder's credit card details and processed transactions after the gateway obtained authorisation from the issuing bank. The gateway operated in such a way that Mr A was unaware of the credit card numbers being used by his customers.

Mr A became suspicious after he received several transactions from the same purchaser in Indonesia, with whom he could not make contact by email or telephone. Mr A contacted the bank for assistance because he was concerned that the matter might involve large scale fraud. He also contacted a number of agencies and organisations including Interpol and the Australian Federal Police but none of the agencies were able to provide him with any assistance.

After more suspicious transactions came through, Mr A asked the bank to let him know what action was being taken and what action he could take. No response was received from the bank.

Mr A then made a number of changes to his website in an attempt to limit fraudulent activity. A program was installed to bar the originators of the suspicious transactions and a time delay was installed to allow only one transaction from the same originating computer to be processed in any one hour period. The additional security measures implemented by the Mr A were ultimately successful.

Mr A complained to the Ombudsman that despite having repeatedly raised the matter with the bank and several other organisations, the bank did not assist him. He complained that the bank terminated his merchant agreement without cause or sufficient notice and then reported him to a credit card scheme and he suffered financial loss as a result.

Bank Response

The bank said that the business appeared on the bank's alert report with excessive chargebacks and it was not required to provide 30 days notice prior to terminating the merchant agreement. It said that it could terminate without notice if it believed that "*the terminal or other equipment is or has been used in a way that may cause losses to us*".

The bank formed the view that there was a significant risk that it could incur large credit card scheme fines as a result of the excessive level of chargebacks, unless it terminated the merchant agreement immediately.

Assessment

The Merchant Agreement

The case manager noted that the merchant is not a party to the agreement between the bank and the various credit card schemes and is not aware of the arrangements between them. For reasons of confidentiality, the bank said it was not at liberty to disclose the credit card scheme rules and therefore in the interests of procedural fairness, it was not appropriate for the case manager to rely on the credit card scheme rules in reaching any determination.

The case manager considered the merchant did all that was required by the bank and the bank conceded that the merchant had been "targeted". She also accepted that the bank would be at risk of loss if the merchant did not maintain sufficient funds in its account for the bank to debit the amount of the transactions that are charged back. In the circumstances, the case manager accepted that the bank had discretion to immediately terminate the agreement.

However, the Ombudsman's decision making criteria not only require him to have regard to the law, but to also have regard to good industry practice, codes of practice and fairness in all the circumstances.

Good Industry Practice

The Ombudsman's banking adviser surveyed four major banks concerning their procedures for monitoring merchant activity and included a question that asked about the banks' usual procedures when they did not suspect merchant involvement in fraud.

The responses of banks surveyed indicated that depending on the nature of the transactions, most banks take steps to educate the merchant in avoiding fraudulent activity rather than immediately terminating or suspending the operation of the terminal. Some banks visit merchants to establish the facts and provide training including videos and best practice brochures to educate the merchant.

Application to this Case

The case manager considered the obligations of the merchant under the merchant agreement and operating guides. She noted that the merchant was required to notify the authorisation centre of any suspicious transactions. A bank newsletter advised merchants that they would be told what to do after they contacted the authorisation centre.

In this case, Mr A went to considerable effort to identify the fraud, notify the bank and other relevant authorities and to independently install measures to protect his business from the targeted activity. Further, in attempting to protect cardholder's details by using the gateway, as required under the merchant agreement, Mr A was unable to monitor and decline transactions so as to avoid the risk of chargebacks.

For its part, the bank failed to provide advice requested by Mr A, after it said that it would, and failed to warn or complain about the manner in which Mr A was conducting his business after being alerted to the fraudulent activity by Mr A. The bank failed to inform Mr A about the consequences of exceeding chargeback thresholds and failed to provide guidance and assistance.

Having regard to the results of the survey and the circumstances of this case, the case manager considered that in immediately terminating the agreement and withdrawing the facility without notice, the bank acted unfairly and contrary to good banking practice. She noted that "*given the serious consequences of termination without notice, there are good reasons to require the bank to exercise its discretion with care and fairness following an adequate investigation including, where appropriate, consultation with the merchant.*"

Conclusion

The case manager concluded that:

1. By not responding to Mr A when he reported the suspicious transactions and requested assistance, the bank failed to act in accordance with its undertaking and representation to provide advice and give guidance to merchants.

2. In the circumstances, the bank acted unfairly and contrary to good banking practice in exercising its discretion to terminate the merchant agreement without notice.

3. It follows that if the termination was unfair, the listing should not have been made. In any event, the merchant agreement did not sufficiently disclose that terminated merchants would be reported to the credit card schemes and included on a database that would be considered by financial institutions in assessing applications for merchant facilities.

4. On balance, but for the disputant's inclusion on the Terminated Merchant's List, Mr A was likely to have been successful in obtaining a merchant facility from another bank.

Both the bank and Mr A accepted the Finding and the bank paid Mr A $1,750.57 for financial loss.

Proportionate Liability for Misleading Conduct

As part of the ninth instalment of the Corporate Law Economic Reform Program (CLERP 9), changes have been made to the *ASIC Act* and the *Corporations Act* to allow for an allocation of liability where there had been misleading conduct in relation to the provision of financial services or a financial product and the claimant has not taken reasonable care. The changes apply to causes of action arising on or after 26 July 2004.

The existing provisions

Section 12DA of the *ASIC Act* provides that a corporation must not, in trade or commerce, engage in conduct in relation to financial services that is misleading or deceptive or is likely to mislead or deceive. The *ASIC Act* deals with financial services where the price of the service does not exceed $40,000, or the price exceeds that amount, the service was of a kind ordinarily acquired for personal, domestic or household use. The price of the service is considered to be the amount paid or payable for the service.

Section 1041H of the *Corporations Act* provides that a person must not engage in conduct in relation to a financial product or a financial service that is misleading or deceptive or is likely to mislead or deceive.

Where there has been a breach of the above sections, the person who has been misled or deceived can bring a claim to recover any loss or damage as a result (See section 12GF of the *ASIC Act* and section 1041I of the *Corporations Act*).

Where a person can make a claim under these provisions, the person's own conduct was not taken into consideration unless they were reckless in protecting their own interests, so that it could be said that the person did not rely on the misleading conduct. This was difficult to show and, as a result, claimants were usually entitled to recover their whole loss. This position remains for causes of action that arose before 26 July 2004.

The new provisions

The CLERP 9 legislation has introduced new provisions into the *ASIC Act*, the *Corporations Act* and the *Trade Practices Act*.

If a person makes a claim for misleading and deceptive conduct that caused economic loss or damage to property, and that loss was caused as a result partly of:

a) The claimant's failure to take reasonable care; and

b) The misleading and deceptive conduct;

then the amount of damages the claimant may recover in relation to the loss and damage are to be reduced to the extent that the court thinks just and equitable, having regard to the claimant's share in the responsibility for the loss or damage. However, a reduction will not be made if the person engaging in misleading conduct did so fraudulently, or with the intent to cause loss and damage.

Concurrent wrongdoers

Where there are two or more wrongdoers and the other wrongdoers have not caused loss or damage fraudulently or with intent, then the changes also allow the court to apportion the loss or damage between the wrongdoers. A court can limit the liability of a wrongdoer to an amount reflecting that proportion of the loss or damage claimed that is considered to be just and equitable, having regard to the extent of the wrongdoer's responsibility for that loss or damage.

This is the case even if the other wrongdoer is not a party to the proceedings, is deceased or insolvent. The provisions do not prevent a person from being liable for the acts of another, for example where a principal is liable for the conduct of its agents or employees.

Application to cases before BFSO

The provisions in the legislation primarily give power to the court to apportion liability where it considers it to be just and equitable to do so. The aim of the Banking and Financial Services Ombudsman Scheme is to provide an independent dispute resolution service having regard to the law, applicable industry codes, good industry practice and fairness in all of the circumstances.

Therefore, in considering disputes that arise on or after 26 July 2004 involving misleading conduct in the provision of financial services, this office will consider whether the claim ought to be reduced because the disputant suffered loss or damage as a result partly of the disputant's failure to take reasonable care.

When does a cause of action arise?

A cause of action for misleading and deceptive conduct has two elements - the contravention of the Act and the suffering of loss or damage. Accordingly, a cause of action accrues not when a breach of relevant legislation occurs, but when the loss or damage is suffered as a result.

Therefore, in applying these changes, this office will look to see whether the loss or damage arose after 26 July 2004, even if the misleading conduct occurred prior to that date.

Future Bulletins on this issue

As the legislation is new and there is no case law at the moment to provide any guidance as to how these provisions will be applied, parties will be invited to make submissions on the applicability of these provisions in relevant cases.

Once this office and the courts have had the opportunity to consider a significant number of cases involving these new provisions, we will issue a further Bulletin on this subject and provide case studies for the guidance of members and their customers.

New Chairman of the Board of BFSO Ltd

I have pleasure in announcing that Professor Michael Lavarch, currently Dean of the Faculty of Law at Queensland University of Technology and former Commonwealth Attorney-General, has accepted the position of Chairman of the Board of BFSO Ltd as of 6 September 2004.

The Board of BFSO has been fortunate to have had the benefit of the capable leadership of Jillian Segal over the past two years. On behalf of the BFSO staff I would like to recognise Jillian's outstanding contribution and thank her for her personal support, her commitment to the Scheme and the vision and energy that she brought to the job.

We warmly welcome Professor Lavarach and I look forward to working with him to ensure the future growth and development of the Scheme.

As always, we welcome feedback on the contents of this Bulletin.

Colin Neave

Colin Neave
Banking and Financial Services Ombudsman