

EMERGING ISSUES IN ELECTRONIC BANKING DISPUTE RESOLUTION

BANKING AND FINANCIAL SERVICES OMBUDSMAN DISCUSSION FORUM OUTCOMES

September 2003

Background

The Banking and Financial Services Ombudsman (BFSO), formerly the Australian Banking Industry Ombudsman (ABIO), is an ASIC approved independent dispute resolution service which considers disputes between individuals or small businesses and financial services providers as defined in the Terms of Reference. The industry members of the scheme include all Australian owned retail banks, a number of Australian subsidiaries of foreign banks, a number of Australian branches of foreign banks and, as from August 2003, non-bank members.

The Ombudsman accepts disputes about electronic commerce, including disputes arising out of online banking transactions that are within the BFSO's Terms of Reference. The BFSO is also the principal dispute resolution scheme for disputes under the EFT Code, which in its revised form covers online and telephone funds transfers.

In March and June 2003, the Ombudsman held a series of discussion seminars in Sydney and Melbourne focussing on issues raised in the Special Bulletin on Electronic Commerce (Bulletin 35 available at www.abio.org.au). The Bulletin discussed some issues emerging in the disputes the Ombudsman has received about electronic commerce, focussing on online banking and credit card transactions, included some case studies and appended a commentary on the investigation obligations of account institutions under the EFT Code. The Bulletin also raised a number of questions of law and practice.



The purpose of the discussion seminars was to take up some of the legal and banking practice issues raised in the Bulletin with a wider audience of in house and external banking lawyers, policy makers and government, consumer and industry representatives.

Each forum featured a principal paper by Professor Alan Tyree followed by a panel and participant discussion. Two articles by Professor Tyree, provide a helpful discussion of some of the issues raised in Bulletin 35.

These are:

- 'Mistaken Internet payments', published in (2003) 14(2) JBFLP 113, and available at <http://www2.austlii.edu.au/~alan/mistaken-epayments.html> and
- 'Riedell gets a credit card', available at <http://www2.austlii.edu.au/~alan/riedell-cc.html>

We are grateful to Professor Tyree and to Mallesons Stephen Jaques for their support of and involvement in the fora.

The other speakers and panel members were:

Sydney: Colin Neave, Banking and Financial Services Ombudsman, Elisabeth Wentworth, General Counsel, BFSO
Andrea Beatty and Andrew Smith, Mallesons Stephen Jaques, Sydney
Louise Sylvan, CEO of the Australian Consumers Association and President of Consumers International

Melbourne: Colin Neave, Banking and Financial Services Ombudsman, Elisabeth Wentworth, General Counsel, BFSO
Jillian Brewer, Case Manager, BFSO
Katherine Forrest and Elizabeth Lanyon, Mallesons Stephen Jaques, Melbourne
Chris Field, Executive Director, Consumer Law Centre, Victoria

Dispute Resolution in Electronic commerce: the context and some general observations

Effective and appropriate resolution of electronic commerce disputes is consistent with wider policy goals of enhancing the uptake by Australians of electronic commerce by increasing confidence and trust. If consumers are confident that any disputes that arise will be resolved effectively and efficiently, they will have increased confidence in using online business and transaction mechanisms.

The focus of the Bulletin and the discussion seminars was a selection of disputes that the Ombudsman had observed as emerging in electronic commerce. It is important to keep in mind the vast number of electronic transactions that take place without problems. It is rare for a system to be perfect and it will be the case that things will sometimes go wrong. What is important is that if a risk of error in particular circumstances is recognised by a bank but tolerated because of, for example, system cost benefits then it is advisable for the bank to translate this into prompt resolution of disputes that arise when the risk is realised.

It is also important, when considering electronic banking to keep in mind that the categories of problems and the legal principles that apply are essentially the same as in the offline environment. In designing electronic banking systems to be used by consumers, established legal principles such as those relating to mandate, mistake and confidentiality together with consumer protection legislation should be kept in mind.

Emerging issues and our approach to them

The following is a brief summary of the emerging issues discussed together with a summary of our approach to them. Our approach has been formulated after consideration of the matters raised in the discussion seminars. In some cases it represents a revision of the views expressed in Bulletin 35.

Issues discussed at the seminars

- System features in conflict with operating authorities leading to the system allowing payments without proper authority;
- Difficulties in recovering Internet banking payments when a mistake is made and the wrong account number is keyed in, despite the correct name being included in the on-screen instructions; and
- Issues to do with chargebacks of credit card payments

System features that are in conflict with account operating authorities

Issue

Particular telephone and Internet payments systems may not accommodate two separate authorisations despite the account operating authorities being 'both to sign'. This limitation may manifest itself when,

for example, a joint loan account is made accessible to telephone and Internet banking. The existing operating authority for redraws on the loan may have been 'both to authorise' but because of system design either one may be able to make a redraw, despite this being contrary to the operating instructions.

Approach

Legal position

A payment made contrary to the account operating authority is in clear breach of mandate and on the face of it the account should be re-credited. The system features are not in themselves a defence to a claim for re-credit of the account. The bank may be able to rely on the equitable legal principle known as the *Liggett* defence but this has been circumscribed in recent times and probably requires some form of unjust enrichment to be proved. See generally Banking Law in Australia, Alan L Tyree, 4th edition para 30.2.

Good industry practice

Existing account operating authorities should be checked as part of the telephone or Internet registration process. System features such as that the system acts on one password should be clearly disclosed and the options given of changing the operating authority to 'either to operate' or blocking telephone and Internet banking.

Account operating authorities should also be checked before linking accounts for the purposes of telephone or Internet banking. Accounts with different operating authorities should not be automatically linked as being able to be operated by a customer simply because that customer's name appears on the operating authority for each account.

Recommendations

Dialogue between the system design, legal and dispute resolution and risk management areas of the bank is essential at an early stage of system development. Apparently there are solutions in place in wholesale banking for recognising more than one password. It would seem desirable to explore the feasibility of using these solutions in consumer banking.

Online transfers to wrong account

Issue

Internet banking screens for online payments commonly require the name, and account number (including the BSB) of the intended recipient's account to be keyed in. Traditionally, the account name has been treated as part of the payment instructions on, for example, a deposit slip and the account name has always been an important part of the instructions for payment of a cheque. Payers often assume that the name and account number for a deposit will be checked against each other before the funds are credited to the payee's account. In practice we know that an electronic transfer is processed solely on the basis of the account number.

This has the effect that, if the payer keys in the wrong account number the payment will be made but to the holder of the account number that has been keyed in. The mistake may only come to light when the intended recipient tells the payer that the payment has not been received. When the payer tries to find out where the payment has actually gone, he or she may be told that the recipient's name cannot be released for reasons of confidentiality. Their bank may claim that it acted on the basis of the instructions it was given, that is, the account number.

The recipient's bank may claim that it has no liability because it acted on the instructions it received from the payer's bank. It may also seek to rely on the Bulk Electronic Clearing System rules (the BECS rules) of the Australian Payment Clearing Association. By the time the payer realises that the payment has gone astray, the recipient may have withdrawn and used the funds, with or without realising that there was a mistake.

Approach

We will consider each case on its facts and take into the account the legal position, good industry practice, any relevant industry code and fairness. We will refer a dispute from the payer to the payer's bank in the first instance. This reflects our view that the first issue to consider is whether the payer's bank was entitled to debit the account, given that the account name and number did not match. The payer's bank may wish to include in its response any relevant information obtained from the receiving bank.

We have revised our approach as a result of the discussion seminars. To date we have focussed on whether there is a misrepresentation by the bank in seeking entry of the account name when it will in fact be disregarded - is there a misrepresentation that both are necessary to effect the transfer? We have also given weight to the practical obstacles for the payer's bank in checking whether the account name and number match. Our revised approach includes considering whether the account has been debited in breach of mandate and other considerations to do with good industry practice.

Legal position

If the account name forms part of the instructions given by the payer to the paying bank then the bank will be in breach of mandate if it debits the account for a payment where the account name and number do not match, and will be liable to re-credit the account. Ordinarily, the account name will form part of the instructions for a payment. This office will take into account terms and conditions stating clearly and prominently that the account name does not form part of the Internet payment instructions and will not be checked. We note, however, and will take into consideration the view of Professor Tyree that such terms and conditions may not be effective at law under, for example, the reasonable fitness for purpose warranty in s 12ED of the *ASIC Act* ['Mistaken Internet payments', at p.3].

If the Internet banking screen requires the account name to be entered, without a clear warning that the name will be disregarded in making the payment and that the bank will rely solely on the account number, then the paying bank may also be liable in misrepresentation or misleading conduct under the *ASIC Act*.

The receiving bank is in a position to check whether the account into which the payment was made matches the account name entered by the payer. It should do so as soon as it is alerted to the alleged mistake. It does not, in our view, breach its customer's confidentiality if it merely confirms to the payer's bank that the account number does not match the name provided by the payer.

The receiving bank is the recipient of a mistaken payment and on the face of it, where the mistake has been verified, it is liable to repay the funds, at least until the point in time that the funds have been withdrawn by its customer and it has, accordingly, accounted to its customer. At this point it also has available to it a defence of change of position. In order to rely on this defence, however, the recipient's bank must show that it has

accounted to its customer. It may be difficult to do this where the recipient refuses consent to disclosure of his or her name and account information and in view of the uncertainty about whether it would be in breach of privacy principles to disclose the information without consent (see further the discussion under 'good industry practice').

The receiving bank is not, in our view, entitled unilaterally to debit its customer's account if the funds have been withdrawn, although it is in the best position to seek the recipient's agreement to repay the funds. It should be remembered that its customer, the recipient, may also have a defence of change of position in good faith.

The receiving bank cannot rely on the BECS rules to avoid liability to the payer for return of a mistaken payment. The BECS rules bind the banks only and do not provide a defence to an action by the payer. As between the banks, however, we note that they do provide for a receiving bank to be indemnified by the sending bank (the payer's bank) for any liability incurred in relying solely on an account number.

Where the paying bank and the receiving bank are the same, and as such, the paying bank is in a position to check that the intended beneficiary's account name and number match, then the bank may also be in breach of a contractual duty to take reasonable care [see *National Australia Bank Ltd v Nemur Varity Pty Ltd* (2002) 4 VR 252].

Good industry practice

In expressing the above view of the law, we recognise that the mistake usually originates from the customer although we do see cases where the bank has unilaterally changed a number or BSB that does not otherwise fit the system. Nevertheless good practice ought to reflect a recognition that both the paying bank and the receiving bank may be liable to the payer and that entry formats for account numbers do not always make it easy to spot a mistake in entry. It is not sufficient, in our view, for the customer to be told to take legal action against the ultimate recipient, particularly as that may have to include preliminary action to discover the identity of that person.

Good practice includes:

- Formatting the entry of the account number to reduce errors so that the number is entered in groups rather than as a single line of digits;

- The recipient's bank seeking clarification of any ambiguity in the instructions, for example, where, because of the mistake, the payment cannot be made without alteration of the BSB or the account number;
- If a customer asserts that a mistake has been made, the payer's bank should notify the recipient bank immediately so that it can verify the mistake and, if there is a mistake, notify its customer, to reduce the chance of inadvertent withdrawal;
- If the mistake has been verified, the recipient's bank should seek its customer's agreement to repay the funds or, if the customer considers that they are entitled to the payment, to disclosure of name and contact details to the payer. If it is the case that the recipient asserts that they are the intended recipient of the funds, it is logical to assume that they accept that the payer will already know their name and account details in order to have effected the payment in the first place;
- What if the recipient refuses to consent to disclosure of his or her name to the payer? There is a good argument that such disclosure is in the legal interests of the recipient's bank and therefore an exception to the duty of confidentiality. The receiving bank must show that it has accounted to its customer and has therefore changed its position in order to resist a claim for repayment of the mistaken transfer of funds. It is less certain, however, whether it would be acceptable under the National Privacy Principles. It is arguable, as suggested by Professor Tyree, that disclosure is permitted under NPP 2.1(a) or 2.1(g). Until the matter is determined by a court or the position is confirmed by the Privacy Commissioner, however, we do not consider such disclosure to be required;
- Giving effect in practice to the agreement contained in the BECS rules that, as between the paying bank and the receiving bank, the payer's bank ought to bear any liability where the account number does not match the account name provided and the account number alone is relied upon.

Recommendations

Professor Tyree suggested in his presentation and paper implementing a system and making the necessary amendments to the BECS rules to allow the payer's bank to check the mandate it receives, as is done in the cheque system. We are happy to participate in discussions about the necessary

amendments or other design solutions aimed at reducing the risks of a wrong number.

Issues to do with chargebacks of credit card payments.

Issue

Bulletin 35 confirmed the view of this office that it is good industry practice for a bank to use available rights under the chargeback rules of the international credit card agreements for the benefit of their customers. This is now an obligation under the revised Code of Banking Practice and, in Professor Tyree's view, represents an obligation in any event, applying by analogy the case of *Riedell v Commercial Bank of Australia Ltd* [1931] VLR 382.

One matter which required resolution was the extent to which banks could request the Ombudsman to take account of specific chargeback rules, given that the rules are confidential and in the absence of permission from the credit card schemes for the Ombudsman to refer to those rules in our decisions.

That matter has been largely resolved by agreement between this office and the credit card schemes, arising from discussions following the discussion fora, to use the chargeback rules in our decision-making and refer to the relevant rule or a summary of it in our decisions.

Conclusion

The purpose of the March and June seminars was to discuss some of the issues emerging in electronic banking disputes and to look for solutions that are consistent with legal principle and good industry practice. If consumers are confident that the disputes that arise will be resolved effectively and efficiently, they will have increased confidence in using online banking.

The participants in the discussion seminars included representatives from private law firms, bank in-house counsel, system, risk management and dispute resolution professionals, representatives of regulators, consumer legal centres and community groups. The level of participation meant that the issues raised could be discussed at an advanced level and in a collaborative way. We thank all the participants for their attendance and

contribution. As always, we welcome any feedback on the issues raised in the Bulletin and this outcomes paper.