4. ensuring that FSR requirements are specifically considered in the project costing and time lines; and
5. implementing a procedure for ongoing FSR compliance monitoring of the software or IT system.

It is essential that financial services organisations regularly audit their IT systems for FSR compliance and implement procedures for considering FSR issues when new technology is brought into the organisation or when existing technology is used in a new way.

Suppliers of financial services technology can add value to an organisation by modifying their products to assist with compliance management. At a minimum, they also need to ensure that their IT products are capable of meeting FSR requirements.

The ongoing impacts of the FSR regime on financial services technology are significant and will continue to play a key role in driving IT system requirements in the financial services industry.

1 The FSR regime is contained in Chapter 7 of the *Corporations Act 2001 (Cth)*.

2 These special regimes may apply, for example, to providers of online trading platforms.

3 Part 7.1, Division 3 of the *Corporations Act 2001 (Cth)*.

4 Section 765A(h)(i) of the *Corporations Act 2001 (Cth)*.

5 Division 6, Part 7.6 of the *Corporations Act 2001 (Cth)*.

6 Such calculators include risk profilers, superannuation, insurance and margin lending calculators, and were common features on websites pre-FSR. The financial services industry body, IFSA, has made a submission to ASIC seeking relief from the personal advice disclosure requirements for these types of website calculators.

7 For example, a Financial Services Guide must be retained for 7 years. See also condition 56 of the Pro Forma 209: Australian Financial Services Licence Conditions, ASIC.

8 Refer to ASIC Policy Statement 164, "*Licensing: Organisational Capacities*".

9 Policy Statement 164 (above), paragraph 125 – 126.

Online transactions between lenders and borrowers – proposed changes to the Uniform Consumer Credit Code

Trudi Lodge & Regina Kho, Allens Arthur Robinson

Trudi Lodge is a Senior Associate at Allens Arthur Robinson, Melbourne. Regina Kho is a lawyer at Allens Arthur Robinson, Sydney. Both are based in the Banking and Finance department and are members of the firm's Consumer Compliance and eCommerce practice group.

Introduction

Consumers are becoming increasingly familiar with online banking, particularly to transfer funds between accounts and pay bills. Banks and other credit providers continue to explore expanding the range of transactions that can be entered into online. Changes are proposed to the Uniform Consumer Credit Code (the **Code**) to make it clear that regulated credit contracts may be formed electronically and documents and notices required by the Code can be given electronically.

Background

Most finance provided to an individual in Australia for a purpose which is not business or investment is regulated by the Code. All lenders must comply with the Code for regulated transactions, and this has had a significant impact on their documentation, computer systems and internal procedures.

Since the Code became law in 1996, lenders have increasingly been considering the possibility of transacting electronically with customers. This has been driven by a number of factors, including increased customer familiarity with online banking and e-commerce generally, a desire among lenders for greater efficiency and the possibility of reducing costs. Recently there have even been moves by government agencies to facilitate electronic transactions, most notably with the initiatives in Victoria and New South Wales towards electronic conveyancing, which follow similar developments in New Zealand.

However, the current drafting of the Code is not conducive to entering into transactions online. In particular, there is uncertainty as to the extent to which electronic transactions are in fact permitted under the Code. Indeed, in certain jurisdictions the Code has been excluded from the scope of the electronic transactions legislation until the status of electronic communications under the Code is clarified.

Current issues with the Code include the following.

- *Issues regarding writing and signatures.* A Code-regulated credit contract is required to be in the form of a 'written' contract document which is 'signed' by the borrower and the lender.[1] It is not clear that an electronic version of the contract document will satisfy the requirement of being in a 'written' form or that the document will be deemed to be signed if a digital or electronic signature is used.

  Similarly, notices from the lender to customers and security providers must generally be in

writing under the Code.[2] Again it is not clear that an electronic version of a notice will satisfy the requirement of writing.

The Code also provides that any post-contract alteration to the credit contract is to be accepted by a borrower by signing or initialling in the margin, however there is currently no express reference in the Code to the acceptance of amendments electronically.[3]

- *Issues regarding formatting.* The Code contains a number of provisions regarding the format of documentation prepared by the lender. For example, the credit contract must be in print size of not less than 10 point.[4]

  Further, certain precontractual information needs to be in tabular format. The issue here is that whilst information might be sent electronically by lenders to customers in the correct format, the receiving computer might amend the formatting.

The Consumer Credit (Qld) Amendment Bill (**Bill**) and the draft Consumer Credit Amendment Regulation (No. 1) 2004 (Qld) (**Regulation**) go a long way towards addressing these and other issues. Unfortunately the Bill won't provide answers to all the practical difficulties faced by lenders.

The Bill confirms that, subject to some specific protections for consumer credit, the electronic transactions legislation in each jurisdiction will apply to the Code. It aims to ensure that consumers who choose to transact electronically are afforded the same level of protection as those who elect to transact via a traditional paper based method. The electronic transactions legislation serves the fundamental principle of technology neutrality by providing that a transaction is not invalid simply because it took place by means of electronic communication. The main proposed changes are discussed below.

Summary of changes

Loan contracts and mortgages

The proposed amendments make it clear that Code-regulated credit contracts and mortgages can be formed electronically, provided the relevant provisions of the electronic transactions legislation are satisfied. The Code requires these documents to be ***written*** and ***signed***.

To satisfy requirements of 'writing' under the electronic transactions legislation, the following must be satisfied:

- at the time the information was given, it was reasonable to expect the information would be readily accessible so as to be useable for subsequent reference; and
- the customer consents to this requirement being met by electronic communication.

In relation to the first of these the Bill goes further than the electronic transactions legislation (see 'Storage and reproduction' below).

These changes will clarify that a document attached to an email, or a document, the text of which appears on a lender's website, can be ***written*** for the purposes of the Code.

The electronic transactions legislation provides that a requirement for a ***signature*** in relation to an electronic message is satisfied if:

- a method is used to identify the person whose signature is required;
- that method indicates that person approves of the message's content;
- that method is as reliable as appropriate for the purpose for which the information is communicated; and
- that person consents to the requirement being met by that method.

The Bill adopts this approach, but makes no specification of what might be "as reliable as appropriate" in the context of regulated lending.

Language and legibility

The Bill amends the provisions of the Code relating to print and type so as to apply only to hard copy documentation. Electronic documentation will, however, be subject to a new provision requiring that credit contracts and notices comply with any additional regulations as to content, legibility and accompanying information. (As regards accompanying information, see 'Presentation of Information' below.)

Storage and reproduction

As indicated above, the electronic transactions legislation requires information communicated electronically to be 'readily accessible so as to be useable for subsequent reference'. The Bill goes further by requiring that the electronic notice or document must be in a format that enables it to be printed or saved and that, at the time the notice or document was sent, it was reasonable to expect that the intended recipient would readily be able to print the notice or document or to save it to an electronic file. This "reasonable expectation" requirement is highly problematic for lenders who will, of course, not know whether the recipient has a printer, has enough memory to save the file, is accessing their email at an internet café which may not have printing facilities, or is using a hand-held device with no print capability. If this requirement is not changed credit providers may need to make reasonably detailed investigations about the hardware and software used by their customers.

Timing and delivery

The Bill also overhauls the notice provisions for electronic communications. It removes specific language relating to electronic communications as such language will be unnecessary when the electronic transactions legislation applies (although reference to 'telex' will be retained to avoid any uncertainty about whether a telex is an electronic communication).

Currently, the Code's provisions governing delivery of notices and

documents do not provide for deemed receipt of documents, but rather that electronic communications are taken to be given on the date they bear, or the date the device from which they were sent records their despatch, whichever is the later. The Bill provides that notices are taken to be given when they are received by the intended recipient. The electronic transactions legislation will determine when an electronic communication is received. It provides that unless otherwise agreed between the sender and the addressee, an electronic message is received:

- when the message enters the information system designated by the addressee; or
- if no information system is designated, when the message comes to the attention of the addressee.

This will effectively shift control of the timing of receipt from the sender to the recipient. While that is consistent with the treatment of electronic transactions generally under the electronic transactions legislation, it does create particular difficulties for Code compliance where notices, copies of documents and other information have to be given within specific time frames. We comment further below on the possibility of lender and borrower agreeing a different regime for deemed receipt of documents and notices.

Presentation of information

The draft Regulation provides that if a credit contract or notice is given by electronic communication, it must be clearly and conspicuously expressed without distractions such as pop up boxes or advertisements. Essentially:

- the text of the document must be capable of being viewed legibly;
- the electronic communication must not contain any image, message, advertisement or the like that is likely to distract the borrower from understanding the document. If there are any such features accompanying or associated with the electronic communication, the lender must ensure that the borrower would be able to easily differentiate those features from the document;
- the document must have scrolling capabilities; and
- the street address and contact number of the lender must be included in the document.

There is, of course, a risk that a customer will not scroll through or read the entire contract before entering into it. The same risk exists, however, with a paper document. The regulators have commented that it would not be technically feasible in all situations to ensure that the borrower scrolls through all relevant information before entering into the relevant credit contract. In their view, the ability for the customer to save or print the document is adequate protection.

Excluded documents

Certain types of documents are not regarded as valid if made, given or provided by electronic means under the Bill and draft Regulation. These include Code-regulated guarantees and notices of default, repossession and demand. It is interesting, however, that if the amendments proceed in the current form, the Code will in fact permit a guarantee to be given electronically *unless* a regulation provides to the contrary. This suggests that the regulators see the possibility, down the track, that guarantees might be able to be formed electronically. If there were a firm policy that electronic guarantees should never be possible, then presumably the new enabling section in the Code itself would exclude guarantees.

What will the changes mean in practice?

Identification – general

One significant issue with purely electronic transactions is that it is difficult for the lender to ensure that:

- it is correctly identifying each customer;
- it is receiving an authentic message from the customer; and
- the electronic message has not been intercepted or altered in transit by some other person.

In particular, there are significant practical issues with purely electronic transactions when dealing with joint borrowers. For example, how does the lender ensure each of them has signified their consent (when entering into a contract or variation) or received information? Issues can also arise with guarantors. While a guarantee cannot be entered into electronically, other documents involving a guarantor can. If a borrower and a guarantor live at the same address, and the lender is seeking the guarantor's agreement that the guarantee extends to an additional advance, how does the lender know it is the guarantor and not the borrower sending an electronic communication in the guarantor's name to agree the extension of liability?

It would therefore be prudent for lenders to employ additional security measures if they do decide to rely on electronic communications with such customers. In particular, it may be that joint borrowers or borrowers and guarantors living at the same address should be required to have separate email addresses to avoid any intentional or accidental deletion of emails addressed to one party by the other.

Identification – anti-money laundering

One major legislative obstacle to transacting with a customer solely by electronic means is the requirement under the *Financial Transaction Reports Act 1988* (Cth) (the **FTR Act**) for a lender to have an identification record for each customer who is a signatory to an account with that lender.[5] This can be either:

- an identification reference; or
- a verification in accordance with the prescribed procedures.

Both methods require the account signatory to produce certain original documents and to sign in the presence of the party giving the reference or undertaking the verification. This means that physical documents will still have to be produced by face to face contact with the customer when identification of a new customer is required.

It is expected these identification and verification procedures will be impacted by the Commonwealth Government's proposed anti-money laundering reforms. The draft Exposure Bill relating to those reforms has not, at the time of writing, been released for comment. However the Attorney-General's Department released an Issues Paper in January 2004 on anti-money laundering reform in the financial services sector.[6] The paper is based largely on the 40 recommendations of the international Financial Action Task Force on Money Laundering dated June 2003[7] and is a useful indicator of the reforms to the FTR Act that can be expected.

It is anticipated that the anti-money laundering reforms will expand lenders' current customer due diligence obligations and increase their reporting and record keeping requirements. At this stage, it is difficult to predict to what extent this will hinder the ability of lenders to transact electronically with customers. However, it is clear that any systems that lenders develop to allow for electronic transactions under the Code will need to comply with the new anti-money laundering legislation, once enacted. This includes lenders who are not currently caught by the FTR Act (which at present only applies to 'cash dealers').[8]

It is also anticipated that under the anti-money laundering reforms financial institutions will be required to exercise a higher level of due diligence where a business relationship is considered to be higher risk. This risk-based approach means that lenders will be required to 'know their customers' and have sufficient detail about their customers' background and business. Sanctions for non-compliance with the new anti-money laundering regime, once implemented, are expected to be heavy.

The anticipated reforms to the FTR Act therefore raise the question of how a lender is to reach a balance in the tension between:

- satisfying its due diligence obligations under the anti-money laundering reforms, once enacted, and safeguarding itself against illegitimate activities; and
- ensuring that those obligations do not interfere materially with electronic transactions with customers under the Code.

Identity - fraud

Fraud is another factor which lenders are increasingly having to address in the on-line environment. Card skimming, identity theft and internet fraud are serious issues for financial institutions.

A report released by the Australian Transaction Reports and Analysis Centre, Australia's anti-money laundering regulator, reveals identity fraud as a growing threat which cost the Australian community $1.1 billion in 2001/02.[9] Certainly, this has been evidenced by a growing prevalence of warnings by financial institutions on frauds and scams.

This increase in identity fraud via paper and electronic means, coupled with existing and anticipated ongoing identification and due diligence obligations for lenders and their agents, suggests that lenders will need increasingly to adopt a cautious approach to the identification and verification of their customers. It will be interesting to see whether, for these reasons, transactions between lenders and their customers continue to involve some form of face to face contact, despite the amendments to the Code to facilitate online transacting.

Signature

The draft changes to the Code do not prescribe what is an adequate functional equivalent for a signature. Reliance on the electronic transactions legislation alone means that lenders are still faced with the difficult question of what form of electronic signature is adequate to identify the borrower, denote his or her approval of the electronic communication and 'be as reliable as appropriate' for the relevant purpose.

To date, there has been much discussion and research into some functional equivalents and methods of identification. These include digital signatures, proxy identifiers such as biometrics and the use of passwords and personal identification numbers (**PIN**s). While digital signatures have been around for a number of years, they are not widely used in the private sector or in a retail environment. Biometric methods such as voice recognition, iris scans and finger printing are being tested but these methods have their limitations due to cost and privacy issues. Passwords and PINs are reasonably widely used as evidence of authority to effect a transaction. There is still a question, however, as to whether they are a functional equivalent of a signature and meet the tests in the electronic transactions legislation.

Lenders will need to carefully weigh the commercial benefit of contracting with customers online against the risks associated with identification and authentication to determine whether they will accept electronic signatures and, if so, what they will use as the functional equivalent of a real signature on paper.

Contracting out of the deemed service provisions

As mentioned above, the deemed service provisions in the electronic transactions legislation will only apply to the extent that the parties have not agreed otherwise. It would be possible for lenders to include different deeming provisions in their credit contracts. The proposed amendments to the Code do not provide that consumers are able to challenge any unfair presumptions concerning the sending and receipt of messages or any unfair contract terms concerning the attribution of a message to them. However, a national working party is currently developing a set of uniform unfair contract terms provisions that could be implemented in all jurisdictions and could apply to the Code.

Version control

If contract terms are provided electronically, lenders will need to ensure that they can prove which version of the terms was applicable at the relevant time. Version control is already a big issue with paper documents. It may become more of an issue if the terms of an electronic document can be readily changed and the changes broadcast or posted instantly to a website.

Unjust transactions

There are some features of online delivery and acceptance of contract terms that may provide additional arguments for a customer seeking to reopen their credit contract on the grounds that the contract, when entered into, was unjust. The court can take into account a number of factors in determining whether a contract is unjust, including whether the lender took measures to ensure that the customer understood the nature and implications of the transaction and, if so, the adequacy of those measures.

In electronic transactions, disabilities, language difficulties or other forms of vulnerability are not easily identifiable. Customers may argue they were not aware that they were in fact entering into a binding contract. These risks can be addressed (although not completely removed) by additional questions and warnings.

The importance of customers being able to distinguish between advertising material and contract terms, and not being distracted by adjacent advertising material, has been discussed above.

Conclusion

The proposed amendments to the Code resolve many of the uncertainties regarding the extent to which documents and notices between lenders and their customers can be made and sent electronically under the Code. There are some technical and drafting issues with the Bill and the draft Regulation. The regulators invited submissions on the draft amendments earlier this year, posing specific questions on which they have invited comment. It is to be hoped that the technical and drafting difficulties will be removed before the Bill is passed. Even if they are, the proposed changes raise their own questions, and do not address some of the key issues lenders will face in practice. In particular, what security measures will lenders adopt where joint borrowers, or a borrower and guarantor, reside at the same address in order to be certain which person the lender is dealing with? Further, how will the changes dovetail with the anticipated anti-money laundering reforms and the likely increase in customer due diligence by lenders? Will the anticipated anti-money laundering reforms hinder the ability of lenders to transact electronically with their customers, or will the anti-money laundering reforms, coupled with general concerns about fraud, be instrumental in ensuring that lenders adopt the most secure systems and procedures for facilitating electronic transactions?

The proposed amendments to the Code go a long way towards increasing the confidence of both lenders and their customers in transacting electronically, and are complemented by the initiatives in the public sector to introduce electronic conveyancing. It will be interesting to see the final form of the amendments once the regulators have had the opportunity to consider the submissions on the Bill, and to see how quickly, once the amendments are implemented, credit providers and their customers will be ready (and willing) to transact online.

1 Section 12 of the Code.

2 See, for example, section 161(3) of the Code.

3 Section 17 of the Code.

4 Section 162(1) of the Code.

5 Section 18 of the FTR Act.

6 "Issues Paper 1 – Financial Services Sector", Attorney-General's Department, January 2004.

7 The recommendations of the FATF can be viewed at http://www1.oecd.org/fatf/pdf/40Recs-2003_en.pdf.

8 The proposal is for the application of the FTR Act to be determined by an 'activities-based' definition, so that any financial institution which provides, deals in or handles a 'financial product' would be caught under the FTR Act. The meaning of 'financial product' is likely to take on a similar meaning to that in the *Corporations Act 2001* (Cth).

9 "Identity Fraud in Australia: An evaluation of its nature, cost and extent", AUSTRAC, 8 September 2003.