FSR impacts on financial services technology

Charles Schofield, Henry Davis York

Charles Schofield is a Senior Associate in the Technology and Communications Group at Henry Davis York, who specialises in technology deployments in the financial services sector.

The new Financial Services Reform (**FSR**) regime came into force on 11 March of this year.[1] The new regime cast a wide net which meant that almost all organisations in the financial services industry had to cope with an overwhelming catalogue of compliance requirements.

Many of these requirements impacted on the technology systems that underpinned those businesses. Organisations spent many months auditing and modifying their information technology (**IT**) systems to cope with the new FSR requirements.

While the main focus for financial institutions to date has been ensuring their compliance with the regime, FSR promises to be an enduring force that is set to have a significant ongoing impact on technology deployments in the financial services sector.

All lawyers and others responsible for compliance or technology in that sector need to have a grasp on the fundamentals of the regime. FSR consequences can be triggered, for example, by introducing new technology into an organisation or by extending the functionality of existing technology.

This article considers the impacts of the FSR regime on financial services technology.

Areas of impact

Financial institutions are heavy users of technology and the FSR regime can have a broad impact on their IT systems. Examples of technology impacted by the FSR regime include:

- online delivery of financial services (eg online applications for products and services or online access to investments or accounts);
- advisory software used by institutions and their representatives (eg modelling tools and calculators);
- trading platforms (eg online share trading);
- non-cash payment systems (eg internet banking and direct credit facilities); and
- technology enabled outsourcing (eg call centres and data processing).

The requirements of the FSR regime can in general terms be separated into three broad categories – licensing, disclosure and conduct related requirements. Each of these categories is considered in more detail below.

Licensing

Under the FSR regime all providers of financial services in Australia need to have an Australian Financial Services Licence (**AFSL**). There are also separate licensing regimes that apply to operators of financial markets and clearing and settlement facilities.[2] The AFSL is, however, the licensing regime with the broadest impact.

Persons who produce 'financial products' or deal in or advise on those products, may need to hold an AFSL. 'Financial products' are defined to include shares and other securities, derivatives, bank accounts, managed funds products, some insurance policies and non-cash payment systems.[3] A significant exclusion from the FSR regime is loans and other credit facilities.[4]

By now all organisations operating in the financial services industry should have addressed their immediate licensing requirements. New licensing issues may arise, however, when an organisation undertakes a new activity, causing it to provide a financial service it is not licensed to provide, or where other parties, which are not primarily financial institutions, become involved in the provision of its services.

Technology can increase the ease by which either of these scenarios may arise. Technology means that logistically it is easier for an organisation to offer its customers a wide range of products, including those of other organisations. Technology can also make providers of technology systems an integral part of the delivery of an organisation's financial services. The impact of the FSR regime and its licensing requirements needs to be considered in both of these scenarios.

For example, a technology enabled distribution arrangement can allow organisations to cross-sell one another's products online. A provider of banking services may, for example, enter into an arrangement with a provider of managed investments to allow bank customers to apply for funds through the bank's website. In these circumstances, the bank needs to consider whether its activities amount to dealing in the funds and, if so, whether its current licence permits that activity.

Similarly, licensing issues may arise where a technology provider becomes involved in the delivery of a financial service. An organisation which processes electronic payments may, for example, require a licence depending on its role in the payment service. Alternatively a provider of a data feed conveying financial information to its customers may require an AFSL if the content of its data feed provides opinions on financial products (e.g. product ratings and reviews).

Coming within the AFSL regime does not mean that an organisation necessarily needs to hold an AFSL. Certain persons can provide financial services as an Authorised Representative (a specially appointed representative registered with ASIC) of an AFSL holder. This involves increased risk for the AFSL holder, as there is a strict liability regime for the

actions of its Authorised Representatives.[5]

In some circumstances, licensing requirements will be a threshold issue for the viability of implementing technology. Obtaining a licence or resolving licensing issues can be a long and expensive exercise and entail additional liabilities. This may add delay and cost to a proposed transaction.

Organisations which intend to use technology to provide financial services or which supply that technology for others to use, need to consider whether there are licensing requirements which impact on them.

Disclosure

The FSR regime contains disclosure requirements which affect organisations providing financial services to "retail clients". This includes many small businesses.

Meeting these disclosure requirements can place significant demands on IT systems. The FSR regime contains stringent requirements about the content of disclosure documents and when they must be provided to a retail client.

There are disclosure requirements that apply when a customer is provided with financial advice, offered a financial product or undertakes certain transactions. Some of these disclosure requirements can be triggered early on in an organisation's dealings with a customer. For example, the requirement to give disclosure documents when providing tailored advice to an individual, arguably applies to online calculators and product selectors, which are available to customers when they browse an organisation's website.[6]

These disclosure obligations, in the context of financial services technology, have their greatest impact on the online delivery of financial services. Organisations providing financial products online, for example, need to ensure that their IT systems are capable of delivering an up to date product disclosure statement to a customer at or before the time the product is offered or issued to the customer.

As a further requirement, organisations need to be able to prove what disclosure was made to a customer, should it ever be called into question. The IT system needs to be capable of recording the disclosure and be sufficiently reliable to permit reliance on its records. This means that relevant systems need to be tested regularly to demonstrate that they are providing disclosure when required, and testing results need to be retained for future proof, if needed.

Certain disclosure documents also need to be retained for a period of 7 years. This is not only a requirement under the Act but also a specific licensing condition.[7] Where the disclosure document is in electronic format, an organisation's systems will need to be capable of storing and retrieving the relevant record.

Technology can also play another part in helping an organisation meet its disclosure requirements. IT systems can be used to prompt compliant behaviour. For example, software used by financial advisers can issue an automated prompt when the adviser needs to make an advice related disclosure. The system can also store records of advice and require acknowledgement that advice has been given before processing transactions. In this way the system can be used to maintain an audit trail with which the organisation can monitor and demonstrate its compliance.

Conduct

The conduct-related obligations under the FSR regime include ensuring that IT systems are of an adequate standard. This is more than just a general requirement, as it is included as a condition of most organisations' AFSL.

ASIC has provided some guidance as to what it considers adequate in the context of IT systems.[8] The main tenor of ASIC's requirements is that the IT systems are secure, current, reliable and robust. This means that problems with maintaining customer records and data integrity may now become AFSL licensing issues.

What is required of the IT system will depend on the complexity of an organisation's operations and the extent to which it relies or ought to rely on technology. Most organisations will also have a range of technology used in a variety of roles.

ASIC has indicated that it expects an organisation to regularly review the adequacy of its IT systems.[9] For most organisations this will require implementing a regular review process jointly run by compliance and IT personnel.

IT systems should also be capable of supporting compliance monitoring. For example, IT systems used in a trading capacity should have sufficient audit trails, note capture and reporting functions to record details of transactions which are sufficient for the system operator to monitor and, if needed, prove compliance with the FSR regime.

Getting it Right

It is important to get it right under the FSR regime as not only will a defaulting financial institution receive unwelcome publicity, but the penalties for failing to comply are significant. Providing financial services without a licence may also mean that a contract for financial services is unenforceable.

Financial services organisations therefore need to carefully consider the impact of the FSR regime when they are procuring or developing software or IT systems to be used in the delivery of financial services.

Planning for any significant technology implementation in the financial services sector should include:

1. a comprehensive initial assessment of the relevant requirements of the FSR regime;
2. ensuring that those requirements are included in the procurement or development specifications;
3. ensuring that contracts with suppliers of IT systems and services contain appropriate commitments as to functionality and performance, so as to permit the financial services organisation to meet the requirements of its licence and, more broadly, the FSR regime;

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