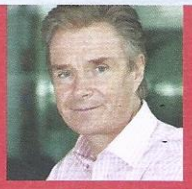
RegulatoryStrategies

The tip of the iceberg

So you think you're FCA compliant...?

Among other things, that must mean you have fully documented systems of control, policies and procedures across your organisation and all your staff have been trained in these. You need to do this as Financial Conduct Authority (FCA) regulated businesses and not doing so will be seen as a significant governance and control risk.



Mike Bradford
Founder and Director, Regulatory Strategies

What goes to the heart of FCA compliance is protecting your data, and demonstrating that you are 'fit and proper' to conduct a regulated business. This isn't new, financial services regulators expect this under the current regime.

Be careful not to approach FCA compliance on 'micro' basis, in other words with a very narrow view of your obligations as you see them purely from a consumer credit perspective. Indeed there is a danger with so much emphasis on the new regulatory regime in the credit press that you will fall into this trap.

A business failure in any high risk area will have the potential to jeopardise your standing in the eyes of the FCA even if it's an area of your business not directly regulated by the FCA, but by some other regulator, for example the Information Commissioner.

For example, anything that suggests you do not have adequate controls around your customer data, as required under the Data Protection Act, will cut right across our FCA compliance requirements.

The data protection world is changing too. You are shortly likely to face having to employ a data protection officer (or outsource this to an external data protection specialist) if you process more than 5000 customer records a year, in other words, most credit businesses.

You will also face:

- mandatory data breach reporting, and the inevitable media coverage and damage to customer confidence this will bring
- more transparent consent requirements for processing credit data making it potentially more difficult to re-use and optimise our customer information
- fines of up to €100m or 5% of our turnover.

That's just the tip of the iceberg of the proposed EU data protection regulation currently being debated in Brussels.

While you have some time to prepare for these data protection changes, the FCA will expect your business to comply with all risk related obligations immediately, including those imposed by the Data Protection Act. This isn't something you can forget about until you see the new regulation.

You need to act now, do you have:

- data protection policies in place
- an up to date privacy policy compliant with cookie regulations
- an incident management plan
- a data retention strategy
- robust contracts in place with third party suppliers that include data protection clauses?

Are your businesses and staff equipped to respond promptly to a subject access request? Do all staff fully understand their data protection responsibilities and have they received adequate training?

If the answer is 'no' to any of the above then it is highly unlikely that the FCA's requirements for conducting a regulated business will be met.

But if you can tick all the boxes, then this will mitigate any regulatory action should the worst happen and for example, you have a data breach or loss, both the Information Commissioner and FCA are likely to be far more punitive on a business without a robust control framework in place, accepting that no business is immune from an incident.

The commercial upside is that businesses which embed data protection in their culture and psyche are increasingly using this as a competitive differentiator, something critical at a time when our industry is under the spotlight on a variety of fronts.

"...both the Information Commissioner and FCA are likely to be far more punitive on a business without a robust control framework in place, accepting that no business is immune from an incident."