



# ARE YOU WATCHING CAREFULLY?

Reporting lines, accountability and governance will become even more critical for consumer credit firms next year, when the Senior Managers & Certification Regime is extended. AMBER-AINSLEY PRITCHARD investigates how the regime will enforce personal responsibility

**T**one from the top – it's a phrase that has entered the common parlance of chief risk officers ever since the Senior Managers & Certification Regime (SM&CR) applied to them. Once regulators forced them to think about the culture of their firms, they had to ensure that an appropriate tone for their company pervaded throughout the entire business – from inception in the boardroom, down to calls with all customers.

Now the same task lies ahead for

consumer credit firms – if they haven't undertaken it already. The SM&CR will affect the personal liability of those who fall within the regime, and some managers of what the Financial Conduct Authority (FCA) calls 'enhanced firms' will find themselves more 'on the hook' than they were under the Approved Persons Regime (APR).

It's yet to be defined how individuals under the enhanced regime could be fined or held more liable. However, the FCA can currently fine individuals who have

controlled functions under the APR. These functions include roles such as directors, chief executives, money-laundering reporting roles and compliance oversight individuals. The number of job functions caught by the SM&CR will only extend as a result of the FCA's consultation on the regime launched last month.

The government aims to extend and implement the SM&CR to all FCA-regulated firms at the start of 2018, according to the consultation, published in July.

The SM&CR was created by the FCA to replace the APR, to “reduce harm to consumers” and to strengthen market integrity by making individuals more accountable for conduct and competence. In October 2015, the Treasury announced its intention to extend the SM&CR to all sectors of the financial services industry, including consumer credit firms. The regime was applied first to banks, building societies, credit unions and PRA-designated investment firms in March 2016. As part of the extension, the FCA proposes three parts to the SM&CR:

- Five conduct rules will apply to all financial services staff at FCA-authorized firms. This set of rules means individuals must act with integrity, due care, skill and diligence, be open and cooperative with regulators, pay due regard to customer interests and treat them fairly, and observe proper standards of market conduct.
- The responsibilities of senior managers will be clearly set out and, should something in their area of responsibility go wrong, they can be personally held to account. Senior managers will be approved by the FCA and appear on the FCA Register.
- Under the Certification Regime, firms will certify individuals for their fitness, skill and propriety at least once a year, if they are not covered by the Senior Managers Regime but their jobs significantly impact customers or firms.

The difference between the Senior Managers Regime and the Certification Regime is that senior managers will have to be approved by the FCA, whereas employees who come under the Certification Regime will only need to be approved by the firm they work for.

Jonathan Davidson, executive director of supervision – retail and authorisations, at the FCA, said: “This is about individuals, not just institutions. The new conduct rules will ensure that individuals in financial services are held to high standards, and that

consumers know what is required of the individuals they deal with.

“The regime will also ensure that senior managers are held accountable both for their own actions and for the actions of staff in the business areas they lead.”

#### Core regime

Announcing the consultation, the FCA said it is committed to ensuring the regime is proportionate, according to the size of the firm, and therefore proposes applying a baseline of specific requirements to all ‘solo-regulated’ firms, called the core regime. A solo-regulated firm is regulated only by the FCA for conduct and prudential supervision, as opposed to being dual-regulated by both the PRA and FCA.

The watchdog said the broad tiers of the regime should apply to all relevant firms,

stating: “This is because the risk to consumers in dealing with badly governed smaller firms is the same as with larger firms.

“Having said that, although our proposals are designed to lead to similar outcomes for consumers, regardless of the firm they deal with, they have been specifically tailored to reflect the different businesses carried out by different persons and allow firms flexibility in how to achieve these.”

#### Differing requirements

The regulator has proposed different requirements for firms with limited scope and larger, more complex firms. A reduced set of requirements will be applied for the group of firms defined as having “limited scope”, which means they currently have a limited application of the APR. The larger, more complex firms that have a greater

#### EXCLUSIVE: THE FCA GRILLED ON REGIME CHANGE

In an exclusive interview with Jonathan Davidson, executive director of supervision – retail and authorisations, at the FCA, *Credit Strategy* delved a little deeper into the consultation.

##### **Q: Will consumer credit firms, through the SM&CR, have to set policies for whistleblowing?**

**A:** “A policy has not been set, and is not going to be set. The FCA hopes and expects that the conduct rules will mean employees will act with integrity.

“It won’t be enough for someone not to report something and just say, ‘my boss told me to do it.’ We hope those working in financial services will blow the whistle if they think something is wrong and listen to their conscience.”

##### **Q: Can individual directors of consumer credit firms be fined now, before the SM&CR is extended?**

**A:** “Under the APR, individual directors can be fined and held to account. The

challenges that had to be addressed in the consultation of extending the SM&CR were two-fold:

Firstly, who has responsibility? Each firm must state who has responsibility for each area and/or function. Prior to this, it was unclear whether it would be fair to fine and hold a senior manager accountable for a junior employee’s action if the action was out of their control.

“We had to consider if we could hold the senior manager accountable for actions reported to them and if the breaches could be foreseen.”

##### **Q: How can we tell if FCA fines against individuals were enabled by the SM&CR?**

**A:** “It isn’t a regulatory requirement to state why individuals have been fined, but I always like to.

“It would be best to inform others in the industry what has been done wrong so they know what mistakes not to make in the future.”





possible impact on consumers will come under the “enhanced regime”. The list below is not exhaustive, but companies that fall under this regime will include:

- Firms with total intermediary regulated business revenue of £35m or more per annum;
- Firms with annual regulated revenue generated by consumer credit lending of £100m or more per annum;
- Mortgage lenders that are not banks, with 10,000 or more regulated mortgages outstanding.

The FCA estimates the number of firms that will be subject to the enhanced regime will be less than one percent of all FCA-regulated firms.

Senior manager functions

As part of the consultation, the FCA has set out the senior management functions, and therefore the senior managers who perform them. It has proposed that all firms, except from limited scope businesses, will have the following job roles classed as senior management functions: Chair, chief executive, executive director, partner, compliance oversight and money-laundering reporting officer.

However, enhanced firms will have additional roles that will be classed as senior management functions, such as chief operations officer. Enhanced firms will also have to create responsibilities maps, along with a single document setting out their management and governance arrangements. Enhanced firms must also have handover procedures, which means ensuring a new person becoming a senior manager has all the information they could reasonably expect, to do their job.

Enhanced firms must also ensure they have a senior manager with overall responsibility for each and every activity, business area and management function of the business.

The FCA said this means a senior manager

“This is about individuals, not just institutions. The new conduct rules will ensure that individuals in financial services are held to high standards”

Jonathan Davidson, director of supervision, FCA

will have primary and direct responsibility for briefing and reporting to the governing body about their area of responsibility. It is designed to prevent unclear allocation of responsibilities, which could result in issues falling between the cracks.

More than one person at a single firm will be permitted to perform a senior management function or certification function. The FCA said this will accommodate people working under a job-share arrangement, adding: “If this was not the case, the proposed rules could be deemed to discriminate indirectly against people who job share, for example, due to family obligations.”

Accountability

Prescribed responsibilities will apply to all firms besides limited scope firms. They are specific functions that firms will need to give to their senior managers to ensure there is an individual accountable for the SM&CR, and key conduct and prudential risks. Prescribed responsibilities include:

- Safeguarding and overseeing the

independence and performance of the internal audit, risk and compliance functions;

- If the firm outsources its internal audit function, taking steps to ensure every person involved in service performance is independent from the people who perform external audit;
- Managing internal stress tests and ensuring the accuracy of information provided to the FCA for stress testing;
- Developing and maintaining the firm’s business model.

A tacit warning

In March this year, the FCA reflected on the one-year anniversary of the regime’s implementation in banks, building societies, credit unions and some investment firms.

The regulator said it has seen firms taking their responsibilities more seriously, but recognises that culture change takes time, so it will continue to keep a “watchful eye” on progress. It said it has been undertaking work to ensure that senior manager responsibilities are properly allocated and understood in firms.

The FCA added: “In some cases, we have seen evidence of overlapping or unclear allocation of responsibilities. In other cases, firms appear to be sharing responsibility among some staff at different levels of management, obscuring who is genuinely responsible.”

On general preparations for the SM&CR, JP Buckley, partner at Shoosmiths, said training is critical to ensure teams both understand the changes and can build the changes into operational practice.

He said: “Financial services firms shouldn’t forget that ongoing compliance needs to be shown, so building tools and processes that are implemented into business as usual and the firm’s behaviours is imperative.”

Jo Pearson, head of risk and compliance at drydensfairfax solicitors, said that businesses will need to decide if the right

people are in the right roles and, if not, what extra training or support is required to help them succeed. She said: “This will hopefully mean further enhancements to existing performance management processes while ensuring proportionality to business size and model.”

Gauging readiness

*Credit Strategy* spoke with firms affected by the extended regime to find out how they are, or will be, preparing for implementation.

Ahead of FCA authorisation, debt purchaser Lowell had taken into consideration the possible implementation of the SM&CR requirements to consumer credit firms.

A spokesperson for Lowell, one of the tens of thousands soon to be subject to the regime, said the SM&CR does not in itself bring any heavy-duty compliance: “It is much about the HR responsibility and managing the necessary controls and documentation to evidence what we should all be doing anyway.”

When asked if the regime could be another driver of consolidation, by enforcing yet more layers of oversight, the spokesperson added: “The ability to better absorb the costs of regulation has always been to the advantage of larger businesses, but it is unlikely to be the sole or primary driver of consolidation in the collections industry.”

As the importance of risk and governance within the debt purchasers has become more evident in the past five years, the role of group chief risk officer is a notable, relatively new position across these businesses.

Lowell recently appointed Bill Flynn, an experienced FCA-approved person and former legal chief within Wonga, who joins in September as group general counsel and UK chief risk officer. The company added that the role of group CRO had already existed within the business before the appointment.



Certification Regime

The Certification Regime is a new requirement that applies to all FCA-regulated firms. This covers people who aren’t senior managers, but whose jobs mean they can have a big impact on customers, the firm and/or market integrity. The FCA won’t approve these people, but firms will need to check and confirm, at least once a year, that these people are suitable to do their job.

The proposed Certification Regime only applies to businesses with employees who perform certain functions, known as ‘certification functions’. These include:

- Significant management function;
- Client asset sourcebook oversight function;
- Functions subject to qualification requirements (for example, mortgage advisers);
- Anyone who supervises or manages a certified function but isn’t a senior manager.

In practice, this means it is possible that in very small firms there will be no one in the Certification Regime if the company only has a handful of senior individuals, who will be senior managers, supported by administrative staff.

From a scale perspective, Pearson said the number of employees that will have to be certified by their firms could be a much bigger population than senior managers.

The FCA’s consultation will be open to comment until November 3 and will publish the final rules in a policy statement next year. But, with the government eager to get the ball rolling with implementation at the start of 2018, it may not be long until we find out how this will affect all firms. **CS**

*The FCA has called on Credit Strategy to emphasise that it is eager to hear the opinions, views and possible side effects this consultation may have on the industry. Feedback can be submitted via: [fca.org.uk/cp17-25-response-form](http://fca.org.uk/cp17-25-response-form)*

“Enhanced firms must also ensure they have a senior manager with overall responsibility for each and every activity, business area and management function of the business”

Financial Conduct Authority (FCA)

# SM&CR and GDPR: Benchmark your preparations

*Credit Strategy*, in association with risk and compliance consultancy Crowe Horwath, is publishing here the results of a reader survey on consumer credit firms' preparedness for the Senior Managers & Certification Regime (SM&CR) and new data protection regulations. MARCEL LE GOUAIS reports



Nearly a quarter of consumer credit firms responding to a reader survey have admitted they are “not prepared at all” for the Senior Managers & Certification Regime (SM&CR).

*Credit Strategy's* survey of a representative sample of consumer credit firms, run in association with risk and compliance consultancy Crowe Horwath, revealed that despite government proposals for the regime to be implemented by all FCA-regulated businesses (including consumer credit firms), during 2018, very few are fully prepared at this juncture.

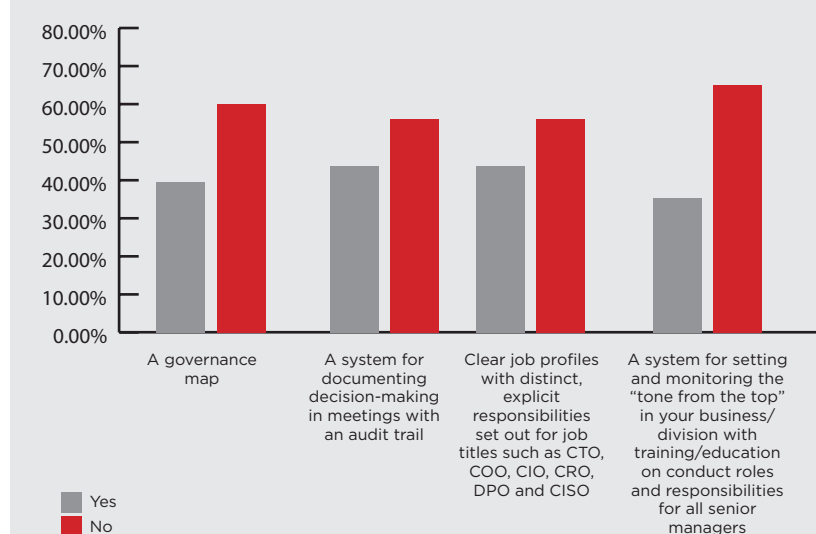
The survey, which posed questions on the SM&CR, the General Data Protection Regulation (GDPR) and cyber crime, found that:

- 23 percent of consumer credit firms were “not prepared at all” for the SM&CR;
- 54 percent admitted they had made “little preparation with a long way to go” for GDPR;
- Nearly a third (28 percent) had not undertaken a thorough test of their IT defences against cyber crime, in the last six months.

The survey also showed that 44 percent of respondents described their current progress on the SM&CR as making “little preparation with a long way to go”. Only six percent said they were completely prepared for the regime, while just over a quarter (27 percent) believe they are now “well prepared.”

The respondents included a mix of consumer credit firms, from peer-to-peer lenders to debt collection agencies, motor

For the SM&CR, have you created any of the following?



finance providers, guarantor lenders and payday lenders.

On more specific SM&CR operational requirements, a general picture emerges that a number of consumer credit firms have more to do. Some preparations though, are well underway; a little under half (44 percent) of the respondents had already created systems for recording decisions in meetings as well as audit trails.

The same proportion of firms said they had created clear job profiles with distinct, explicit responsibilities set out for job titles such as chief technology officer, chief operating officer, chief information officer,

chief risk officer, data protection officer and chief information security officer.

However, 60 percent of firms had not yet created a governance/responsibilities map and 65 percent had not created a system for setting and monitoring the “tone from the top” in their business/division, with training or education on conduct aspects linking to the roles and responsibilities for all senior managers to evidence embedding of the appropriate culture.

As *Credit Strategy* reports this month (see p18), how this tone from the top and business culture is set at board level – and how it filters down into every facet of the

company – is at the crux of what the SM&CR is designed to cultivate.

The regime will hoist personal accountability for directors up to unprecedented levels within thousands of consumer credit firms. And this is just part of the rationale for the survey.

The GDPR – we shouldn't have to explain what it is at this late stage – will also enforce a level of personal responsibility for a wider range of roles hitherto not experienced.

Senior directors and managers therefore face a convergence of regulatory requirements that will crystallise next year. The survey seeks to establish where consumer credit firms are on their journeys toward implementing both the SM&CR and the GDPR.

Amid rampant cyber crime attacks on financial services and telecoms giants, the survey has also yielded insight on how robust consumer credit firms believe their systems are against this growing threat (see next page), but first and foremost, the questions focussed on the levels of preparedness for regulatory change. For the first time, there's a barometer to measure your position against others in the same boat.

Both the GDPR and SM&CR, inevitably, carry new operational exposures and hazards, and some 44 percent of participants said they had “good awareness” of the potential risks brought on by the SM&CR. A total 13 percent said they had “full awareness” of the dangers, but interestingly a higher number (17 percent), said they had “no awareness”.

Awareness and progress on GDPR, the survey showed, is further ahead.

## GDPR

May 25 is the deadline for implementation – it's handy having a date clearly set in advance. As one would expect of a highly ambitious project to ensure uniform levels of

data protection across EU member states, the operational requirements are vast and in most cases for retail banks are being managed by special project teams. Higher penalties also come into play; the ICO will have powers to fine firms up to four percent of global turnover or up to as much as €20m.

Severe penalties seem to have only been a marginal motivating factor though, with 54 percent of participants still admitting that they've made “little preparation and still have a long way to go”. Another eight percent worryingly said they were “not prepared at all”.

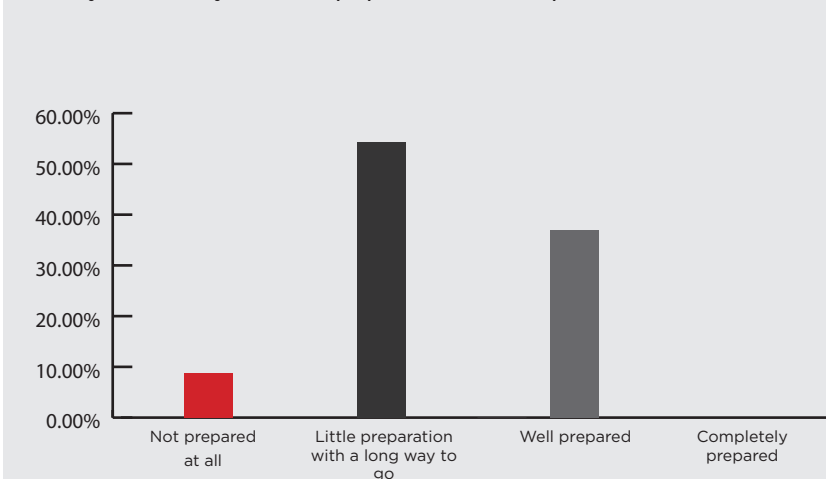
On the other hand, a relatively healthy number are forging ahead, more than a third (37 percent) said they're “well prepared” for implementation by May 2018. Perhaps unsurprisingly, and a sign that some are both progressing but still need guidance, none

said they were “completely prepared”.

When it comes to the basics of HR aspects and operations, these have largely been done. Some 74 percent of firms had already appointed a data protection officer and 57 percent had reviewed their data subject access request policy and process. But broadly, some of the tougher challenges have not yet been overcome; 59 percent had not ensured at board level that their data subject consent process will be valid in future and 76 percent had not yet undertaken any privacy impact assessments, where automated processing is carried out.

As part of the survey, participants were also asked how confident they were in the preparedness of their third-party service providers (debt collection agencies, business processing outsourcers and law firms), for GDPR. Some 15 percent simply didn't know, 30 percent had little confidence, six percent

Full compliance with GDPR regulation needs to be implemented by May 2018. How would you describe your level of preparedness for its implementation?



had no confidence, but most (40 percent) had a reasonable level of confidence in those on their panels.

### Cyber crime

At times this year, it appeared from the rapid succession of major scale cyber security attacks that few financial services firms, if any, could have complete confidence in their systems.

However, 54 percent of consumer credit companies responding to the survey said they had a reasonable level of confidence in the robustness of their systems to protect customers' personal data. Even 30 percent had complete confidence and only four percent admitted they had no confidence. However, despite the rapid agility in how cyber crime attacks evolve, nearly a third (27 percent) of respondents said they had not undertaken a thorough test of their IT systems' defences, and reviewed contingency plans to prepare for a cyber attack, in the last six months.

### Preparation acceleration

Looking ahead at the operational and compliance requirements coming in next year, data protection officers and risk directors will emerge as business critical roles, if they're not already. 2018 will be the year of personal accountability.

Combined, the GDPR and SM&CR will reconstruct how customer data is managed, protected and made available for consumers, as well as establishing how critical decisions are made and documented, so that individual senior managers are 'on the spot' should the expected standards not be achieved. There will be no finger-pointing, 'it wasn't me' defences. The penalty for getting either of the regimes' requirements wrong will be more severe than ever. We can all expect the implementation progress so far to accelerate into the new year. **CS**

As part of GDPR implementation have you:



### RICHARD WARRINGTON, SENIOR EXECUTIVE, CROWE HORWATH:

"On July 26 the FCA issued its consultation paper, CP17/25, extending SM&CR to all regulated firms and it is clear the FCA wants to encourage a culture where staff at all levels take personal responsibility for their actions.

Firms must put in place governance structures and responsibility maps that make it absolutely explicit where responsibility lies, so that across each firm the position is fully understood. There is no hiding place should questions be raised regarding customer treatment or customer outcomes not meeting regulatory expectations.

"The SM&CR will take effect during 2018 and the opportunity to provide feedback to the FCA is available, but there is no doubt, SM&CR will be rolled out, so now is the time to prepare and ensure responsibilities are allocated and all parties know what that means to them.

"With regard to GDPR, the date is set and the ICO has said there will be no extensions, so firms must understand how they handle customer data and in particular, what it is used for. Undertaking a privacy impact

assessment is a sensible starting point; ensuring data subject access request procedures are tightened up; and reviewing how consent is obtained – these are all critical elements and are harder to achieve under the new regulations.

"Once again, not implementing adequate procedures, with robust governance and oversight, will put firms at risk of serious sanctions (if not fines). It is imperative that all consumer credit firms move on very soon from 'little preparation with a long way to go', otherwise time will run out and the ICO will not view that position sympathetically.

"In the same way, complacency is your worst enemy when it comes to the risks of cyber crime. Firms may feel well-protected, but how do you know? When was the last time a full penetration test was carried out? Cyber criminals are always one step ahead, so how far behind might your defences be?"

• Crowe Horwath Global Risk Consulting is supporting firms in all areas covered by the survey. Contact [richard.warrington@crowehorwathgrc.com](mailto:richard.warrington@crowehorwathgrc.com) / 012 4223 4421 / 020 3457 6659.