ADVICE MATTERS

The CPD Solution For Financial Professionals

fstp
financial services training partners

In this issue

1hr of structured CPD Accredited by The London Institute of Banking & Finance

Industry updates | Key factors for your business | Better Interviews with your clients | Technical know how

FSTP in partnership with

unicorn an access company

ComplianceServe

2019 | Vol 7 | Edition 7

Welcome to edition 7 of

ADVICE MATTERS

Hello once again from the Advice Matters Team at FSTP.

This month we have been out and about with the FCA and very interesting it has been too.

First of all we attended one of the FCA's round table road shows which centred on the impact of RDR on advice and what the FCA could do more of to help the industry. No surprises when I tell you the main feedback was that RDR had widened the advice gap and educating the public about financial services in general and the importance of receiving professionals' advice was where the attendees saw the FCA could help the industry most. Interesting that the most recent advert on pension scams shows the 'scam adviser' having the time of his life on someone else's hard-earned pension pot but doesn't tell people what to do to ensure they are dealing with a bona fide adviser!

The theme ran on at the rather noisy FCA annual meeting, when amongst the questions that FSTP partners asked on SM&CR and culture there were many from disgruntled individuals and groups on how they had been on the receiving end of less than professional and ethical treatment by those firms that aren't compliant or don't act in the spirit of FS regulation.

Our three articles this edition, **Product oversight and governance**, **The FCA Annual Report** and **GDPR one year on** plus a number of the links to press releases, speeches and statements all resonate with the stance on understanding how to put the customer at the heart of what you do and doing it, and that includes the FCA.

We hope you enjoy this edition. As always feedback is welcome.

For those of you going on holiday or staying at home we hope the sun shines.

All the very best

The Advice Matters Team
at FSTP

ApEx Standards

The learning outcomes and the ApEx Standards can be found at the end of this edition of Advice Matters

Next month

We will focus on:

- Pensions update
- Financial promotions
- Supervising certified people

Recognised CPD programme

The London Institute of Banking & Finance

Staying on Track

This section will keep you up to date with the changes in market, product, legislation & regulation.

Product oversight and governance

> We will do work this year on new product governance and research unbundling... All that work is a product of our supervisory work as to how effective the application of MiFID II has been.

Andrew Bailey
CEO, Financial Conduct Authority
Speaking to the Treasury Select Committee – 15/01/19

Mr Bailey's stated commitment to the Treasury Select Committee was set in stone with publication of the FCA's Business Plan for 2019/20 in April. The regulator will be looking for firms to demonstrate they are taking product governance and oversight seriously and embedding them into the way they do business, especially when introducing new products and/or services to the market.

With that in mind, it seems like an opportune moment to refresh our memories about some key aspects of product oversight and governance, as well as the associated regulatory requirements and expectations.

What is product oversight and governance?

To begin with, the phrase, 'product oversight and governance' refers to the systems and controls that a firm has in place to design, approve, market and manage a product throughout its lifecycle to ensure that it meets legal and regulatory requirements.

According to the FCA, good product governance should result in products that:

1. 1. meet the needs of one or more identifiable target markets;
2. 2. are sold to clients in the target markets by appropriate distribution channels; and
3. 3. deliver appropriate client outcomes.

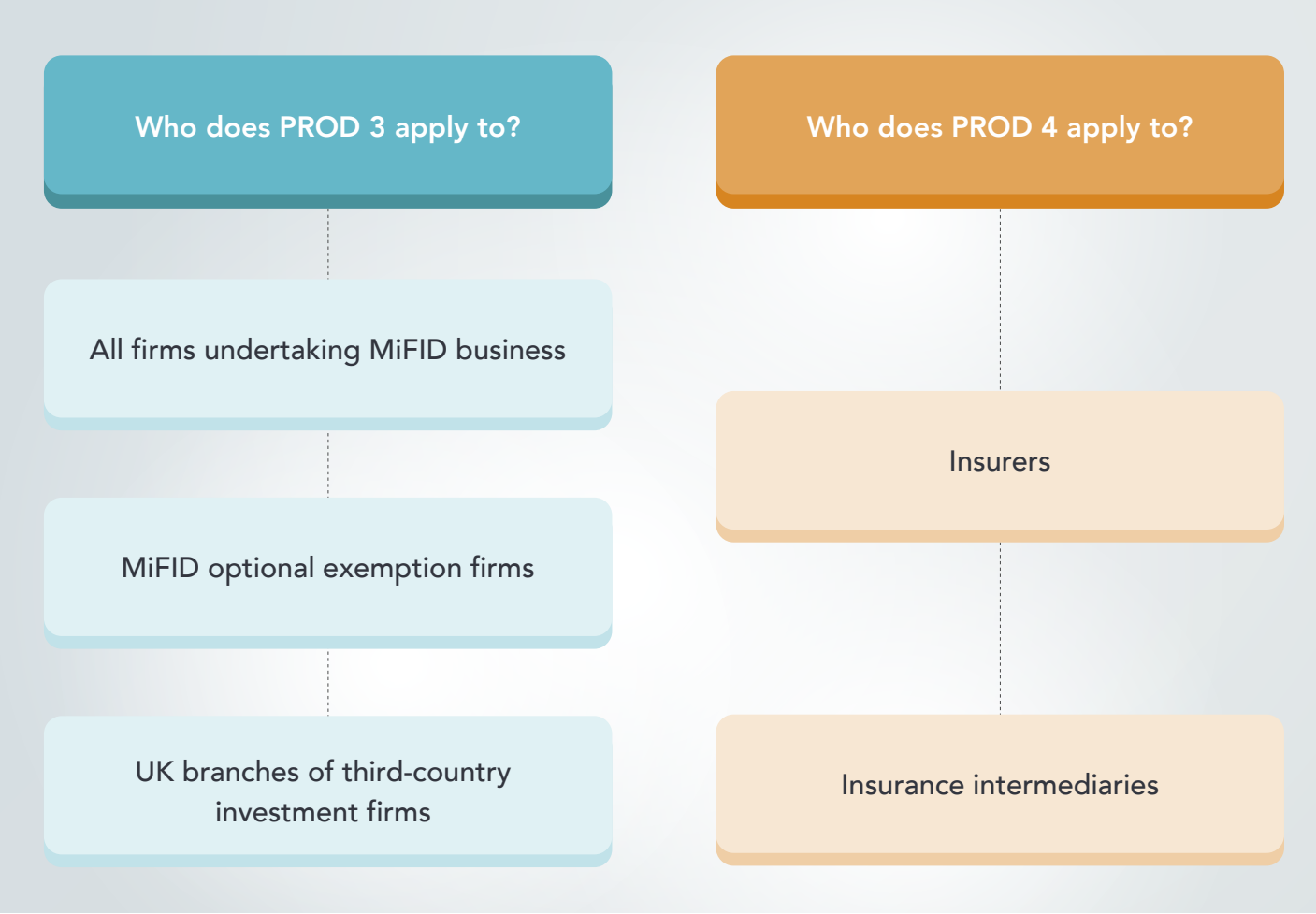
The rules and guidance relating to product oversight and governance can be found in the Business Standards chapter of the FCA Handbook, within PROD – the Product Intervention and Product Governance Sourcebook – which is made up of 4 sections:

PROD 1 -General application and purpose – inc. application of PRODS 2, 3 & 4

PROD 2 - Statement of policy re: the making of temporary product intervention rules

PROD 3 - Product governance: MiFID (manufacture/distribution of products and investment services)

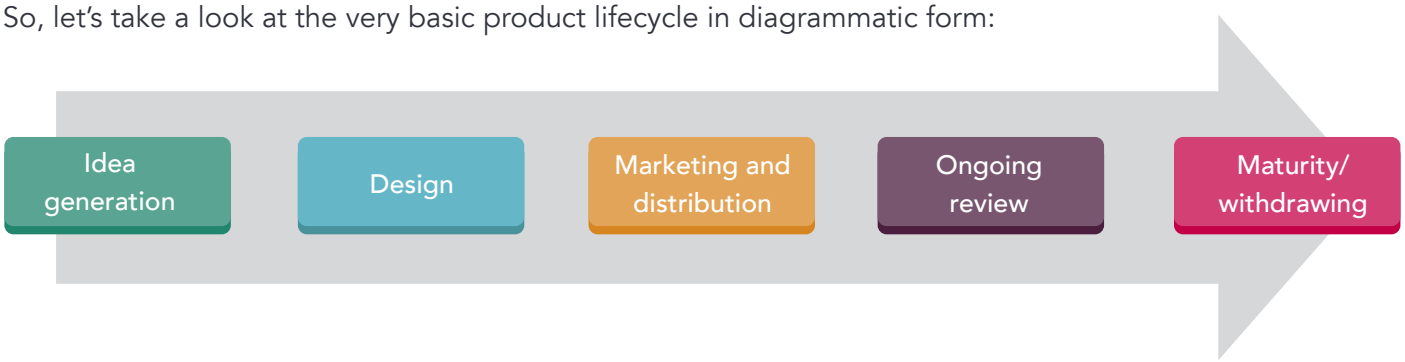
PROD 4 - Product governance: IDD (manufacture/distribution of insurance products)



When addressing their approach to PROD compliance, firms should take the following steps:

- Establish a product oversight and governance process, that reflects what actually happens in practice and can be audited.
- Allocate Board-level accountability for product governance and compliance oversight.
- Ensure that staff possess relevant knowledge and experience of products and services.
- Select appropriate distribution channels.
- Monitor performance and suitability of existing products.
- Maintain transparent escalation procedures for taking action as and when issues are identified.

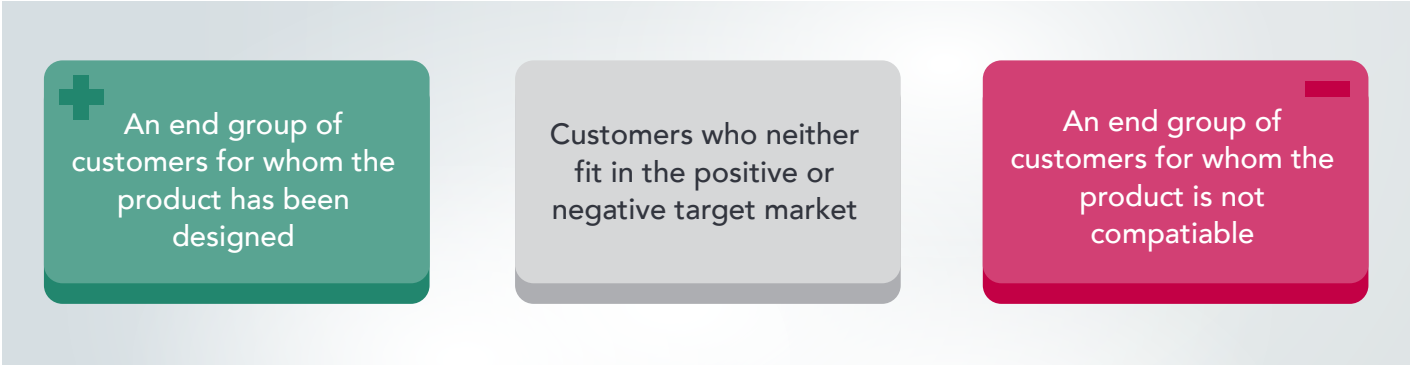
So, let's take a look at the very basic product lifecycle in diagrammatic form:



Idea generation – determining the target market

Within the idea generation phase sits one of the most important aspects of product governance, namely identification of the **target market**. This is likely to be at the forefront of any FCA review of the systems and controls surrounding firms' oversight and governance of their products and services.

Whether it's a manufacturer, or a distributor, a firm should be able to demonstrate that it has identified the product's target market – i.e. the customer group(s) that it is suitable for – known as the **positive target market**. This process should also identify any group(s) for which the product is unlikely to be suitable – the **negative target** market.

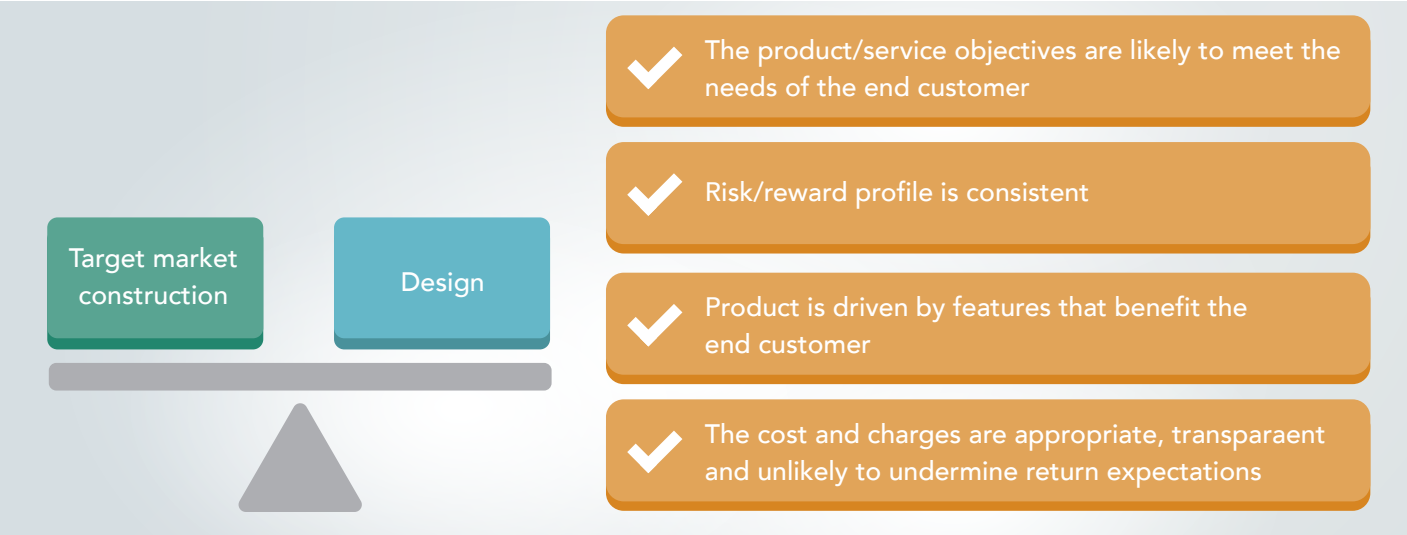


When identifying the target market, the following factors should be taken into account:

Type of customer	i.e. retail, professional and eligible counterparty
Knowledge and experience	required of the end customer for them to understand the product
Financial situation	of the end customer, focusing on their ability to bear losses – i.e. the % loss the end customer should be able and willing to afford (or maximum proportion of assets that should be invested)
Risk tolerance	of the end customer, e.g. speculative, balanced, conservative – terms used should be clearly defined
Customer objectives and needs	the product is designed to meet, including reference to time frames

Design

Investing time in identifying and understanding the target market will pay dividends when it comes to the next stage in the product lifecycle – namely, **design**. In fact, the firm's control mechanisms should not allow the design phase to start until there is sufficient and appropriate evidence of the proper construction of the target market.



Marketing and distribution – manufacturer/ distributor communication

The effectiveness of communication between manufacturers and distributors is likely to be another area that the FCA will pay particular attention to in its forthcoming review.

Product manufacturers should ensure that they are sharing all appropriate information on their products and services with those who distribute them.

This should include such things as:

- details of product/service being offered
- target market description
- appropriate distribution channels
- costs and charges
- materials' approval process (if appropriate).

When communicating with a distributor, a manufacturer should take into consideration a number of factors including:

- the distributor's likely level of knowledge and understanding of the product
- the information required and preferred delivery medium, or combination of media (e.g. face-to-face discussion, written material, web-based, etc.)
- whether the distributor will be producing its own marketing materials
- any restrictions on the use of the materials required (e.g. 'for professional clients only').

Communication invariably involves a two-way exchange and the product governance and oversight process is no exception to this principle. A distributor should be prepared to provide a product manufacturer with key information such as:

- the volume of sales made
- the customer type making use of the product/ service
- whether the product/service has been sold to any customers outside the target market
- customer complaints received about the product/service.

Ongoing review – compliance monitoring

To be truly effective, it is essential for any framework of governance and oversight to stipulate regular independent monitoring, or review.

In the context of product oversight and governance this means that a manufacturer should take steps to determine whether the products and services it has put out to market remain fit for purpose and operating as intended in line with the expected requirements of the target market.

The results of this monitoring should inform the manufacturer's internal discussions and decision making in relation to the product strategy and any changes that may be required to this.

The review should provide the manufacturer with early feedback of potential issues identified by distributors and end customers, with any lessons learned being incorporated into the continually evolving product governance process.

The firm's compliance function should be responsible for providing independent monitoring and reporting on the product governance process and the reports generated from this activity must be made available to the FCA, on request.

Distributors should also be conducting regular reviews of products and services to confirm that they remain in line with the target market's needs. In doing so, if problems are identified (e.g. sales being made in the negative target market exceed a pre-defined volume threshold) changes must be made as appropriate and the manufacturer made aware of these.

Product review and compliance monitoring play such a fundamental role in facilitating effective product governance and oversight, it is more than likely that soon they, too, will also be subject to closer scrutiny by the FCA.

So, product governance and oversight is a subject on which the FCA places great emphasis and it is unsurprising that the regulator should be planning to look at how well (or not!) the industry has responded following MiFID II's introduction.

Maturity/withdrawing

If you're concerned by the prospect of the FCA's scrutiny of your product governance and oversight arrangements, you may be able to take some heart from the results of the regulator's 2018 review of product governance in the retail banking sector, which set out to assess:

- how firms identify and respond to risks from their customers' changing needs and external factors
- whether firms' product governance frameworks provide sufficient challenge to their risk assessment assumptions
- how product reviews identify potential customer harm, provide effective management information and use customer feedback

From this thematic review, the FCA found that:

- All firms had product-focused committees to discuss product issues and make decisions.
- Staff holding Senior Management Functions were involved in all stages of the decision-making process and were clear about their accountabilities.
- All firms used a product governance framework that covered all stages in the product lifecycle, including policies and procedures for product design, launch and product reviews – these frameworks were being continually developed and improved.
- Product design processes appeared to be established and embedded, although this was less convincing in relation to product review processes.
- All firms' product review processes included capturing feedback from existing customers.

The following areas for improvement were identified:

- None of the firms tested customer understanding.
- Some firms needed to strengthen their product review processes to ensure they act on any identified lessons or risks, e.g. recording the outcome of product reviews more clearly.

Richard Galley, FSTP's Learning Director, is the author of the above article and delivers the courses detailed in the link below. If you would like more of an insight into how your firm should be addressing product oversight and governance these courses will do just that.

https://www.fstp.co.uk/course/product-management-and-governance19/

https://www.fstp.co.uk/course/product-management-governance-for-insuranceoctober19/

Tech Check

In Tech Check we address aspects of technical knowledge that you need to keep abreast of and that will enable you to have better conversations with your clients.

The FCA Annual Report

The FCA has published its Annual Report and Accounts for the year 2018/19.

Aside from the bald figures around how the regulator is paid for and where the money is spent, there are some nuggets of information that those in the regulated sector should take heed of. Following close on the heels of the Business Plan, this document identifies issues found throughout the previous year and gives hints as to where it will be looking next. The last thing you want to hear from the regulator is 'I told you so'.

Executive overview

The Chair of the FCA, Charles Randell, is positive in his analysis of the roll-out of the Senior Managers Regime to larger regulated firms, but he recognises that the extension to smaller firms is a major part of the next stage of the FCA's transformation. As in previous years, technology and the internet are highlighted for their impact on individuals through financial scams – the FCA seeks to develop its own use of technology to respond through more sophisticated supervision and enforcement in this area. Over 520 warnings were issued regarding unauthorised firms, a 59% increase over the previous year.

Recognising the focus that the FCA has recently placed on the regulated activities in larger firms, the Chair is keen to emphasise there may have been a perception of gaps in the implementation of their overall remit. It is with this in mind that the FCA sought to increase understanding and foster new discussion around the scope of the FCA through the publication of a new report, published at the same time as the Annual Report and Accounts.

Andrew Bailey, the Chief Executive, has taken the opportunity to highlight the efforts of the FCA in dealing with Brexit. Obviously, the FCA has been looking at worst-case scenarios including how a no-deal Brexit affects its priority to ensure that consumers and the integrity of UK markets remain protected as far as possible.

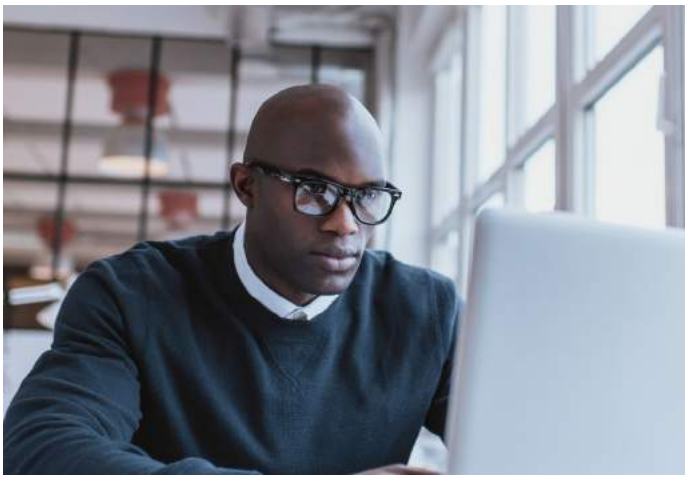
Following the transition of around 1000 firms from the Claims Management Regulator to the FCA and the introduction of restrictions to charges for high-cost credit activities, the FCA recognises that all has not gone smoothly in this sector in the past. In addition, Andrew Bailey has indicated that final rules are due later in the year to address problems for around 140,000 mortgage customers that have been disadvantaged by the FCA's own current regulation.

Cross-sector priorities
Customer outcomes and enforcement

This has been a 'good' year for enforcement – the eye-watering fine of £102 million for Standard Chartered Bank's failing in AML procedures and nearly £33 million for Santander relating to deceased customer funds emphasise the FCA approach to failures in regulatory compliance. In times where the FCA is requiring personal responsibility through the Senior Managers and Certification Regime, individuals should take note that breaches continue to be punished severely.

The regulator continues to push positive outcomes for customers, and if it must do that through fines, at least firms can't say they haven't been warned over the years.

On a related topic, the PPI claim deadline is approaching, and the FCA is claiming credit for increasing the number of PPI enquiries to 8.4 million in the past ten months. Hopefully this will mean the end of adverts featuring the disembodied head of the 38th Governor of California.



What is noticeable in the report is an increasing focus on pensions once again. Final rules and guidance arising from the Retirement Outcomes Review are expected soon, as is research on the level of savings required in retirement. In addition, the FCA has now expressed concern that advice on pension transfers remains very poor, with around half of all advice given considered unsuitable.

Unfortunately, then, perhaps the words of the Cyberdyne Systems Series T-800 will continue to resonate across our TV screens. As it said (on numerous occasions) – 'I'll be back'.

Expansion

With an increased remit over recent years (claims management, consumer credit, etc), the FCA has recognised that its current premises and staffing model is inadequate. There is a commitment to double the FCA presence in Scotland to cover expansion in retail lending, investment and intermediaries, as well as the level of casework with financial advisers, wealth managers and pension scams.

One area of note is the extension of the Financial Ombudsman Service and the DISP complaint handling rules to larger SMEs. Since 1 April 2019, SMEs with annual turnover below £6.5m and either a balance sheet below £5m or fewer than 50 employees have been able to refer complaints to the Ombudsman. Larger charities and trusts, as well as a new category of personal guarantors, are also now eligible for the service.

3500 staff members have moved to new premises in Stratford with the aim of reducing costs and implement some 'green' efficiencies.

Although whistleblowing reports have maintained at a steady level of 1100 per annum, the FCA plans to increase staff in the dedicated whistleblowing team and has rolled out additional internal training in this area. It is interesting to note that less than 1 % of whistleblowing reports required significant action by the FCA to mitigate harm, and less than 10% in total required any action by the FCA, although there remains a large proportion of cases still being considered.

EU

There is no doubt that the ongoing EU withdrawal saga has placed a range of pressures on the staff and the planning ability of the FCA. When a key objective of the organisation is to 'protect and enhance the integrity of the UK financial system', one must have (some) sympathy for the planners and teams involved.

EU withdrawal has been its number one priority and the FCA has been working closely with the Treasury to minimise the impact of a no-deal Brexit. Ongoing interaction with EU regulators and other bodies has allowed a Temporary Permissions Scheme to be prepared alongside other tools which allow EEA firms to continue to operate here under their existing passports for a time.

Accountability

The Senior Managers and Certification Regime (SM&CR) continues apace, with the aim of ensuring that senior staff know exactly what they are accountable for and that every individual within a firm takes responsibility for their own behaviour.

Having moved from banking, through insurance and now to the wider regulated sector, this is a step change in how the regulator ensures the right thing is done by the right people. Although there remains consultation work outstanding, the FCA has now indicated that the status of legal functions within a firm may be excluded from the regime.

In March 2019, the FCA introduced plans for the 'Directory' – a new public resource for checking the details of a wider group of people working in financial services, including those certified by firms to provide important services to customers, such as financial advice. This will be launched to the public from March 2020 through an enhanced consumer portal.

Financial Crime

Alongside this document, the FCA have published an 'Anti-Money Laundering Report' (**https://www.fca.org.uk/publication/corporate/annual-report-2018-19-anti-money-laundering.pdf**). The report highlights the FCA promotion of the use of regulatory technologies and data analysis to detect activities like market abuse. In May 2018, the FCA held an International Anti-Money Laundering and Financial Crime "TechSprint" focused on how new technology can be used more effectively to combat money laundering and financial crime. The next TechSprint (July/August 2019) will examine the potential to improve information-sharing to detect and prevent financial crime.

The 'Office for Professional Body AML Supervision' (OPBAS) began work within the FCA in January 2018 to oversee the quality of professional bodies' supervision of legal and accountancy firms. OPBAS completed its first round of supervisory assessments and published its anonymised findings in March 2019. It has also established an Expert Working Group between the National Crime Agency and the accountancy bodies to enable them to collaborate and share information and intelligence.

In addition to the efforts made by the FCA in regulating this area, it identified some weaknesses in oversight provided by Professional Body AML Supervisors, including the accountancy sector and many smaller professional bodies. The FCA claim they focus more on representing members interests rather than supervising and enforcing standards. The FCA will actively seek engagement with these bodies for intelligence sharing and expert working groups.

Alongside this, the FCA is reviewing several areas highlighted for improvement in combatting money laundering in the UK. These were raised by the international, intergovernmental organisation, the Financial Action Task Force (FATF).

Perhaps two of the fastest moving areas with potential for customer harm (through crime or misrepresentation) are the continuing growth in crypto assets and crowdfunding. The FCA Peer to Peer policy statement was published in June and we can expect more from them on cryptos following the expected Treasury report in the autumn. With 1% of all global crypto trade passing through the UK and increasing numbers of both applications and scams getting passed to the regulator, this is not going away.

At an individual customer level, the FCA now claims over ½ million people have visited its ScamSmart website this year.

Data security and computing

The FCA has been pushing awareness of the increasing numbers of technology and cyber incidents affecting UK financial services. In 2018, there was nearly a 200% increase in this area, year on year. They believe that a large part of the increase is due to awareness, rather than increased exposure, but recognise this as a world-wide threat.

This is highlighted by their participation in GFIN (the Global Financial Innovation Network) launched in January 2019. GFIN is an international group of financial regulators and related organisations who will facilitate testing in the regulated space across different jurisdictions, allowing a joined-up approach to regulation and customer security.

The financial system's increasing reliance on technology and data and the outsourcing of systems to specialist companies, is, however, seen as a particular threat to smaller firms. To aid in this, the FCA has now published additional information on how to improve its cyber resilience. This is available on its website.

In addition, the FCA has indicated that although FinTech can help firms to deliver better financial products, lower costs and be more inclusive, it also has the potential to quickly spread problems or system errors, causing customers harm. This emphasis on customer impact should be taken as a sign of increasing oversight and control from the regulator.

Through a discussion paper issued in summer 2018 by the FCA, the PRA and the Bank of England, options were considered on how to strengthen firms' operational resilience to cyberattacks and other disruptive operational incidents. The industry can expect a consultation paper on this area this year.

The FCA also says that it recognises the benefits of cloud computing through cost savings and faster deployment cycles, but is concerned around the risks to data privacy and the cross-border infrastructure in place with many firms. Expect this to feature in the consultation paper.

Sector priorities
Wholesale financial markets

The FCA has advised that last year's plan to publish an 'Approach to Market Integrity' document has been postponed in light of EU withdrawal and the resources it has needed to dedicate to it. This is now something for the future and will obviously affected by the final outcome of Brexit.

The ongoing monitoring focus in this area seems to concentrate on:

- Increased monitoring of financial markets to reduce illegal activity. The recent 'Financial Crime Guide for Firms' clarifies expectations.
- Continuing monitoring of new MiFID II rules will take place, and firms should take heed of the FCA finding published in April on 'payment for order flow' (PFOF).
- Weaknesses identified in operational resilience reviews throughout the industry last year mean that this will remain a priority for the foreseeable future.

Investment Management

The FCA highlights the industry has also undergone significant regulatory change recently, including MIFID II, PRIIPs and the Asset Management Market Study. These areas can expect review over the coming year, although, once again, the effects of Brexit may have dramatic consequences on how this goes forward outside of Europe.

A couple of years ago the FCA referred the investment consulting and fiduciary management sector to the Competition and Markets Authority (CMA) for a full market investigation. At the end of 2018 the CMA proposed remedies and a plan to bring the rules for fiduciary management into the FCA's Handbook. This will be a large task – consultation papers to be expected.

Pensions and retirement

The FCA continues in its work to produce a joint regulatory strategy with The Pensions Regulator (TPR) which sets out a vision for the medium to long term. This can be split in two, the strategic review of the entire consumer pension's journey; and how the FCA can drive value for money for pension scheme members.

On a more immediate basis, the regulator has highlighted through its ScamSmart figures that people concerned about pensions and retirement income scams have soared over recent months. This is contrasted by a reduction in the percentage of people actually seeking professional advice in this area.

Retail banking

Change continues apace in the retail banking world. Ring-fencing came in for larger banks and PSD2 and open banking are expected to drive banking innovation. The FCA has already commented on the number of technology firms that have started to enter the payments market.

The coming year can expect a real focus on the implementation of Standards on Strong Customer Authentication (SCA-RTS) and Common Secure Communication (CSC). These changes to security around payments and online banking bring a range of modifications to how customers bank (e.g. two-factor authentication). The run up to September 2019 implementation will be under scrutiny.

Ongoing fraud is also under the spotlight here, too. PSD2 reporting is to be used to tailor FCA monitoring – figures on fraud reporting will be available to the industry in September.

Retail lending

Lending to customers that is affordable and appropriate for their circumstances is a priority in this sector, and focus is being particularly placed where vulnerable customers may be affected.

Monitoring and expectations continue to evolve in retail lending following the FCA taking responsibility, however it is interesting to note that emphasis has been placed on the following expectations arising from the creditworthiness policy document published in November:

- the distinction between affordability and credit risk
- ensuring that credit assessments are proportionate
- the role of information about consumers' income and expenditure
- the need for clear and effective policies and procedures.

The mortgage market is still seen as a difficult area to compare products and the FCA is pushing for innovation here, and this seems to be an opportunity for someone in the FinTech world. The FCA also criticises the restrictions within its own guidance, hindering competition. I think we can expect some change to MCOB.

The motor finance sector can expect increased scrutiny following investigation into the use of commission models and the incorrect use of pre-contract disclosure.

General insurance

On a positive note, the FCA has stated that its investigation into the wholesale insurance broker market did not seem to pose significant levels of harm to consumers. On a less positive note, it was not happy with potential conflicts of interest, the level of information disclosed to clients and the contractual arrangements between brokers and insurers. I think that we will see some action to ensure these specific topics are covered in future compliance visits.

Other areas picked out from recent reviews in the distribution network as having issues include GAP insurance, travel insurance (particularly for vulnerable customers) and tradesman insurance. The FCA advises that closer supervision will follow.

Retail investments

London Capital & Finance PLC dominates the regulator's thinking in this area and the potentially criminal aspect of the saga. Monitoring of compliance in the high-risk and complex investment sector is obviously coloured by that.

On the 'business-as-usual' side, this year there has been a focus on an analysis that combines the Retail Distribution Review and the Financial Advice Market Review outcomes. The FCA plans to use this analysis to assess the future of the market for advice and other guidance services. Industry input is sought, but change is expected.

Skills & Expertise

Personal development is often forgotten or neglected, as it is not seen as important as the other areas of CPD. In reality it can be the aspect that makes the real difference to your clients and your earning capacity. In each edition of Advice Matters we will discuss potential development areas and ensure any regulator focus that aligns to this area is covered in a very timely manner.

GDPR One Year On

How long would it take you to spot a data breach? How soon would it take you to inform the Information Commissioner about it?

Under the GDPR, companies have just 72 hours to notify the supervisory authority of data breaches. But it wasn't always like this.

Pre-GDPR, companies took – on average – 60 days to uncover data breaches.

These surprising findings were uncovered by cybersecurity provider Redscan, following a FOI request made to the ICO and analysis of 182 data breach reports.

> "The fact that so many businesses failed to provide critical details in their initiative reports ... says a lot about their ability to pinpoint when attacks occurred and promptly investigate the impact of compromises."
>
> Mark Nicholls
> **Director of cyber security at Redscan**

There was some good news though. Financial services and legal services performed slightly better, taking on average 16 and 20 days to report incidents.

So, what do we know so far on the GDPR journey and where should the focus be?

In this article we will focus on a few key areas:

- data breaches;
- transparency and consent;
- request from data subjects
- enforcement action
- ongoing GDPR compliance

Data breaches

Not surprisingly, EU Data Protection Authorities (DPAs) have seen a sharp increase in the number of data breaches being reported to them since "mandatory" breach notification was considerably extended at the end of May 2018.

In the UK the Information Commissioner, Elizabeth Denham, gave a **speech** to the International Privacy Forum on 4 December 2018 in which she said that the Information Commissioner's Office (the ICO) had received over 8,000 notifications of data breaches since the end of May 2018.

That is compared with just 3,311 notifications between 1 April 2017 and 31 March 2018, and 2,565 between 1 April 2016 and 31 March 2017.

The numbers alone show us how seriously the subject is now being taken. However, despite this sharp increase in notifications we are only just starting to see the drip down of enforcement action.

In the same ICO blog the following extract gives us a clear insight into what to expect moving forwards: a clear insight into what to expect moving forwards:

> "The focus for the second year of the GDPR must be beyond baseline compliance – organisations need to shift their focus to accountability with a real evidenced understanding of the risks to individuals in the way they process data and how those risks should be mitigated. Well-supported and resourced DPOs are central to effective accountability.
>
> Strong accountability frameworks are the backbone of formalising the move of our profession away from box ticking. They reflect that people increasingly demand to be shown how their data is being used, and how it is being looked after. They are an opportunity for data protection to be an enabler of growth and innovation whilst building people's trust and confidence in the way their information is handled."

The recurring themes of transparency and consent

Transparency and consent continue to be a regular feature of complaints to DPAs.

One of the key themes arising from these complaints is the level of detail that is expected to be included in the transparency information provided to data subjects. For example, in its statement on the Google fine, the CNIL said that Google's

> "purposes of processing are described in a too generic and vague manner", and "that the information about the retention period is not provided for some data."

Beware and be warned!

Requests from data subjects

GDPR granted individuals more extensive rights in relation to the use of their personal data, including the right to data portability. It also gave lots of noise to the existing rights of erasure and access.

There are two types of data subject access requests (DSAR) that are particularly problematic to firms:

1. The first is the one that asks lots of complicated questions about data processing, some which fall within scope of Article 15 of the GDPR and others which do not. These requests are manageable, if somewhat time consuming but often require experienced data protection professionals to avoid response pitfalls.
2. The second category is requests by employees and former employees for data contained during work activities, mainly in the form of emails. These are again time-consuming and expensive exercises that businesses need to conduct.

What fines have we seen so far?

2018 was a busy year for the ICO...

The Information Commissioner's Office (ICO) issued the most – and largest – fines ever in 2018, including:

- 11 fines totalling £1,290,000 to organisations for serious security failures
- 11 fines totalling £138,000 to UK charities for unlawfully processing personal data in the 12 months to March 2018.

But, do not forget the maximum penalty in 2018 was £500,000, issued to both Facebook and Equifax.

Facebook was slapped with the £500,000 fine for its role in the well-documented Cambridge Analytica scandal. The information of 87 million Facebook users was improperly shared with the political consultancy through a quiz that collected data from participants and their friends.

Facebook was found guilty of allowing application developers access to user information without sufficient consent, failing to make suitable checks to secure personal information and not taking action once the misuse of data was discovered.

Note – Facebook is now preparing for a $5 billion fine from the US Federal Trade Commission over violations of its 2011 consent decree with the agency.

Equifax was fined £500,000 after failing to protect the personal information of up to 15 million UK customers during a cyberattack. Hackers stole personal data including names, dates of birth, addresses, passwords, driving licences and financial details. The company had retained data **for longer than necessary**, making it vulnerable to unauthorised access. Longer than necessary is a key tenet of the GDPR to be aware of – you must be able to prove reasoning on this matter.

The systems compromised were actually based in the US, but because the UK branch failed to ensure its American parent was protecting UK customers, the ICO was forced to issue the fine.

Post GDPR the attention-grabbing fines handed out by the ICO include:

- Mobile network company EE has been fined £100,000 by the Information Commissioner for sending customers over 2.5 million text messages last year without permission. The texts were meant to encourage customers to use its app and upgrade their handsets, which EE said it considered service messages rather than marketing. The ICO ruled, however, that messages that include promotional material are subject to electronic marketing rules, which can draw fines of up to £500,000.
- International hotel group Marriott is facing a £99m fine after hackers stole the records of 339 million guests. The Information Commissioner's Office issued a notice of its intention to fine the group for infringements of the General Data Protection Regulation (GDPR) for the 2014 hack on the Starwood hotels group – two years before it was acquired by US-based Marriott.
- British Airways has said it intends to contest a record £183m fine over a 2018 data breach.

Remember, under the GDPR, companies can now expect fines of up to:

- €10,000,000 (£8.8 million) or 2% of total global annual turnover (whichever is higher) for lesser data breach incidents.
- €20,000,000 (£17.6 million) or 4% of total global annual turnover (whichever is higher) for significant data breaches.

The headline GDPR fine so far has been the **€50 million fine** by the French DPA (CNIL) against Google for lack of transparency, inadequate information and lack of valid consent in relation to its use of personal data for the purposes of personalising advertisements.

That fine is significantly higher than any of the other fines imposed by any EU DPA for breaches of the GDPR so far.

The CNIL justified the amount and the publicity of the fine on the basis that:

- Google would (continue to) infringe essential principles of the GDPR: transparency and consent;
- the infringements were not a one-off, nor were they time-limited; they are still ongoing;
- the scale of the infringement would be significant (thousands of French people are affected); and
- Google's economic model would partly be based on the personalisation of advertisements, and therefore it is of utmost importance that Google complies with its obligations in that respect.

So, where does this leave us and what should we be thinking about now?

It is safe to say that 2018 was a busy year in the world of data protection and privacy, but it shows no signs of slowing down into 2019 and beyond. Enforcement activities have slowly unfolded and will take some time.

To avoid falling foul of the GDPR, and with more than 12 months of new guidance, learning and best practices and enforcement action to go on, it's a good time to carry out an audit of your current compliance.

Where are you in your compliance plan and what more can be done?

Here are just five things to be considering (both now, and on an ongoing basis):

1. Policies and procedures

Check whether your existing policies and procedures need updating as a result of new guidance or business expansion and changes.

If your compliance activity last year was relatively limited, consider whether your current suite of policies and procedures needs extending to ensure an ongoing culture of data protection responsibility.

2. Customer/supplier relationships

Review and review again your contracts with your clients, vendors, and third-party suppliers. Do they comply with the requirements of the GDPR, including the rules on transferring personal data outside the EU? If not, how will you go about amending them?

3. Privacy impact assessments

Do you understand the circumstances in which you are required to undertake a privacy impact assessment? If so, do you have a framework for carrying them out? Privacy impact assessments are a key part of the GDPR's philosophy of privacy-by-design.

4. GDPR training

Are you rolling out annual GDPR refresher training, with more advanced training for employees that regularly handle personal data (such as the sales and marketing, HR and IT teams)?

DPAs take training seriously and it is usually one of the first questions they ask when things go wrong.

5. Security breaches

Consider whether your employees really know what to do if there is a security breach or if a DPA commences any enforcement action.

Preparing for the worst case scenario will help you to take defensive steps to mitigate the serious reputational and financial consequences that can follow when things go wrong.

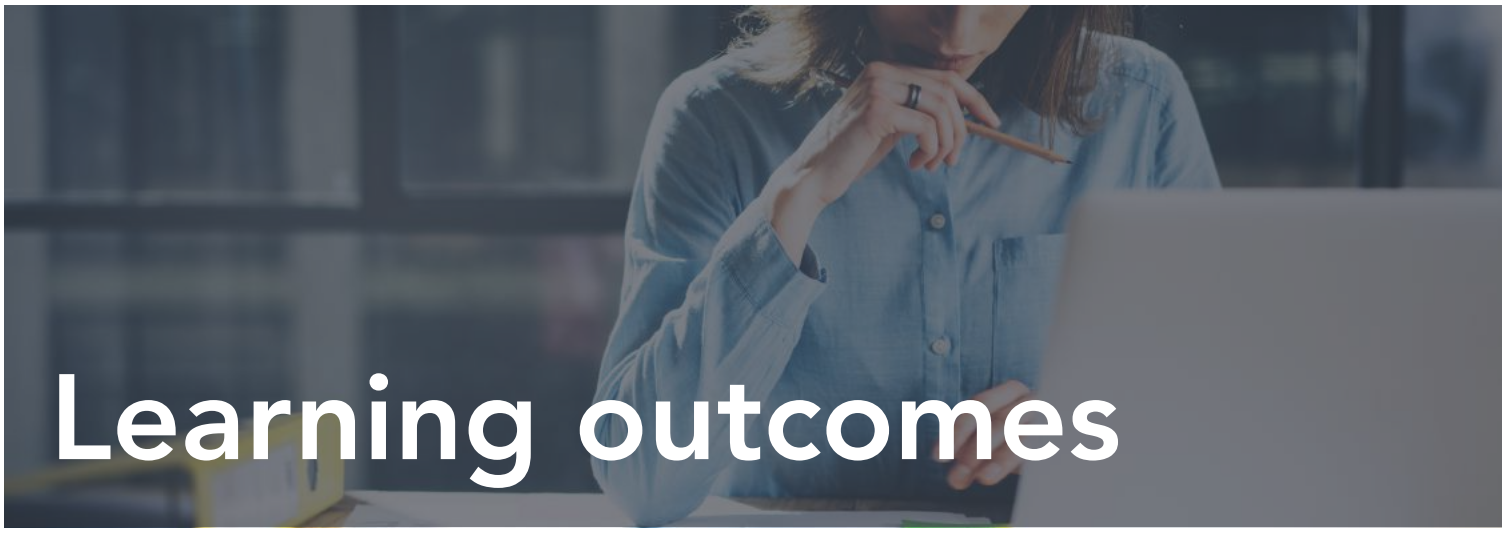
Links to FCA documents

July 2019

Relevant consultation papers (CP), policy statements (PS), guidance consultations, finalised guidance, press releases, speeches, statements, news stories and discussion papers

Reference	Title	Link
Press Release	Two found guilty of insider dealing	https://www.fca.org.uk/news/press-releases/two-found-guilty-insider-dealing
Press Release	FCA confirms permanent restrictions on the sale of CFD's	https://www.fca.org.uk/news/press-releases/fca-confirms-permanent-restrictions-sale-cfds-and-cfd-options-retail-consumers
Speech	Andrew Bailey speech at the FCA conference on intergenerational differences	https://www.fca.org.uk/news/speeches/andrew-bailey-opening-speech-fca-conference-intergenerational-differences
Press Release	FCA bans the sale of crypto derivatives to retail consumers	https://www.fca.org.uk/news/press-releases/fca-proposes-ban-sale-crypto-derivatives-retail-consumers
Speech	Speech on the FCA's changing strategic priorities for the pensions sector	https://www.fca.org.uk/news/speeches/changing-landscape-fcas-strategic-priorities-pensions-sector
Press Release	FCA's Annual Report	https://www.fca.org.uk/news/press-releases/fca-publishes-annual-report-and-accounts-2018-19

Reference	Title	Link
Statement	Statement on the FCA's finalising rules on SM&CR	https://www.fca.org.uk/news/statements/senior-managers-and-certification-regime-finalising-fca-rules
Press Release	HSBC agrees to extend the redress scheme to customers impacted by historical debt collecting practices	https://www.fca.org.uk/news/press-releases/hsbc-agrees-extend-redress-scheme-customers-impacted-historical-debt-collection-practices
Press Release	Richard Baldwin is convicted of money laundering	https://www.fca.org.uk/news/press-releases/richard-baldwin-conviction-money-laundering
Press Release	FCA sets out its priorities for 2019/20	https://www.fca.org.uk/news/press-releases/fca-sets-out-its-priorities-2019-20
News	New platform to replace Gabriel	https://www.fca.org.uk/news/news-stories/new-platform-replace-gabriel-improve-collect-data
Speech	Andrew Bailey speech at the annual public meeting 2019	https://www.fca.org.uk/news/speeches/andrew-bailey-speech-annual-public-meeting-2019
Speech	Charles Randell – speech at the annual public meeting 2019	https://www.fca.org.uk/news/speeches/charles-randell-speech-annual-public-meeting-2019



Learning outcomes

By reading this edition of Advice Matters and applying the learning you will be able to:

Understand the key aspects of product oversight and governance
Clarify the regulators expectations when creating new product and services
State where you can find the rules and guidance on product oversight and governance in the FCA Handbook
Confirm the steps a firm should take when addressing its approach to PROD compliance
Understand the scope and the remit of the FCA; how it's changing and how it may change in the future
Discuss the implications of regulator enforcement
Acknowledge the re-emphasis on pension advice
Understand the extension to FOS and DISP compliant handling rules to larger SME's
Be aware of how the FCA are dealing with whistleblowing
Know the various bodies the FCA are working with in their fight against financial crime
State the specific areas the regulator is focusing on for the various financial service sectors
Explain the effect of GDPR interaction
Recognise the reoccurring GDPR themes
Consider the difference in reporting figures to the ICO pre and post GDPR implementation
Discuss the fines for non GDPR compliance
Verify what your GDPR compliance plans should consist of

The ApEx standards

The ApEx standards addressed in this edition of Advice Matters are:

Core or specialist subject	Learning outcome	Indicative content
FSRE	The regulation of financial services	• The role of the Financial Conduct Authority (FCA), • The role of other regulating bodies such as the Competition Commission, the Office of Fair Trading, the Pensions Regulator, the Information Commissioner. • Financial Services and Market Act (FSMA) 2000, other relevant legislation. • The role of EU regulation and relevant directives • Additional oversight – senior management, trustees, auditors, external compliance support services.
FSRE	The FCA's responsibilities and approach to regulation	• Statutory objectives and how FCA is structured to achieve these: – powers and activities – financial stability and prudential regulation – powers to deal with financial crime. • Risk based supervision, discipline and enforcement, sanctions to deal with criminal activities.
FSRE	The principles and rules as set out in the regulatory framework	• Regulated activities and authorisation requirements. • Approved person and controlled function responsibilities. • Record keeping, reporting and notification requirements. • Professionalism and the training and competence requirements. • Anti-money laundering and proceeds of crime obligations. • Data protection including data security. • Complaints procedures and responsibilities to customers. • The Financial Ombudsman Service (FOS). • The Financial Services Compensation Scheme (FSCS).

Training Courses | Training Consultancy | Board Services | CPD Programmes | E Learning | Coaching Services

unicorn an access company | ComplianceServe | Chartered Banker | CISI ACCREDITED TRAINING PARTNER | The London Institute of Banking & Finance