Chapter 10

The Small Firms Financial Crime Review (2010)

10.1 Introduction

10.1.1 **Who should read this chapter?** This chapter is relevant, and its statements of good and poor practice apply, to **small firms** in all sectors who are subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R and small **e-money institutions** and **payment institutions** within our supervisory scope.

10.1.2 In May 2010 the *FSA* published the findings of its thematic review into the extent to which small firms across the financial services industry addressed financial crime risks in their business. The review conducted visits to 159 small retail and wholesale firms in a variety of financial sectors. It was the first systematic review of financial crime systems and controls in small firms conducted by the *FSA*.

10

10.1.3 The review covered three main areas: anti-money laundering and financial sanctions; data security; and fraud controls. The review sought to determine whether firms understood clearly the requirements placed on them by the wide range of legislation and regulations to which they were subject.

10.1.4 The *FSA* found that firms generally demonstrated a reasonable awareness of their obligations, particularly regarding AML systems and controls. But it found weaknesses across the sector regarding the implementation of systems and controls put in place to reduce firms' broader financial crime risk.

10.1.5 The review emphasised the key role that the small firms sector often plays in acting as the first point of entry for customers to the wider UK financial services industry; and the importance, therefore, of firms having adequate customer due diligence measures in place. The report flagged up concerns relating to weaknesses in firms' enhanced due diligence procedures when dealing with high-risk customers.

10.1.6 The *FSA* concluded that, despite an increased awareness of the risks posed by financial crime and information supplied by the *FSA*, small firms were generally weak in their assessment and mitigation of financial crime risks.

10.1.7 The contents of this report are reflected in ■ FCG 2 (Financial crime systems and controls), ■ FCG 3 (Money laundering and terrorist financing), ■ FCG 4 (Fraud), ■ FCG 5 (Data security) and ■ FCG 7 (sanctions and asset freezes).

10.2 The FSA's findings

10.2.1 You can read the findings of the *FSA's* thematic review here: http://www.fsa.gov.uk/smallfirms/pdf/financial_crime_report.pdf

10.3 Consolidated examples of good and poor practice

10.3.1 Regulatory/Legal obligations

Examples of good practice	Examples of poor practice
• A small IFA used policies and procedures which had been prepared by consultants but the MLRO had tailored these to the firm's business. There was also a risk assessment of customers and products included in an MLRO report which was updated regularly.	• An MLRO at an IFA was not familiar with the JMLSG guidance and had an inadequate knowledge of the firm's financial crime policies and procedures.
• One general insurance (GI) intermediary had an AML policy in place which was of a very good standard and included many good examples of AML typologies relevant to GI business. Despite the fact that there is no requirement for an MLRO for a business of this type the firm had appointed an individual to carry out an MLRO function as a point of good practice.	•

10.3.2 Account opening procedures

Examples of good practice	Examples of poor practice
• A discretionary portfolio manager had procedures that required the verification of the identity of all beneficial owners. The firm checked its customer base against sanctions lists and had considered the risks associated with PEPs. Most new customers were visited by the adviser at home and in these cases the advisers would usually ask for iden-	• An IFA commented that they only dealt with investment customers that were well known to the firm or regulated entities. However, the firm had some high risk customers who were subject to very basic due diligence (e.g.: copy of passport). The firm said that they were concerned about the high reputational impact an AML incid-

tity verification documents on the second meeting with the customer. Where business was conducted remotely, more (three or four) identity verification documents were required and the source of funds exemption was not used.

ent could have on their small, young business. The firm stated that they would deal with PEPs but with appropriate care. However, the firm did not have a rigorous system in place to be able to identify PEPs – this was a concern given the nationality and residence of some underlying customers. The firm appeared to have reasonable awareness of the sanctions requirements of both the Treasury and the United States Office of Foreign Assets Control (OFAC), but there was no evidence in the customer files of any sanctions checking.

- A venture capital firm had policies in place which required a higher level of due diligence and approval for high-risk customers. However, they had no system in place by which they could identify this type of customer.

10.3.3 Monitoring activity

Examples of good practice

- A credit union used a computer-based monitoring system which had been specially designed for business of this type. The system was able to produce a number of exception reports relating to the union's members, including frequency of transactions and defaulted payments. The exceptions reports were reviewed daily. If there had been no activity on an account for 12 months it was suspended. If the customer was to return and request a withdrawal they would be required to prove their identity again.
- A Personal Pension Operator's procedure for higher risk customers included gathering extra source of funds proof at customer take-on. The firm also conducted manual monitoring and produced valuation statements twice a year.
- Within a GI intermediary firm, there was a process where, if a customer made a quick claim after the policy has been taken out, their records were flagged on the firm's monitoring system. This acted as an alert for any possible suspicious claims in the future.

10.3.4 Suspicious activity reporting

Examples of poor practice

- One MLRO working at an IFA firm commented that he would forward all internal SARs he received to SOCA and would not exercise any judgement himself as to the seriousness of these SARs.

	• At an IFA the MLRO did not demonstrate any knowledge of how to report a SAR to SOCA, what to report to SOCA, or how to draft a SAR. The firm's policies and procedures contained a pro forma SAR but this was not a document the MLRO was familiar with. • An IFA was unaware of the difference between reporting suspicions to SOCA and sanctions requirements, believing that if he identified a person on the Consolidated List he should carry on as normal and just report it as a SAR to SOCA.

10.3.5 Records

Examples of good practice	Examples of poor practice
• An advising-only intermediary firm used a web- based system as its database of leads, contact names and addresses. It also stored telephone and meeting notes there which were accessed by staff using individual passwords.	• A file review at an IFA revealed disorganised files and missing KYC documentation in three of five files reviewed. Files did not always include a checklist (We expect that KYC information should be kept together in the file so that it is easily identifiable and auditable.)
• A home finance broker classified customers as A, B or C for record keeping purposes. A's being Active, B's being 'one-off or infrequent business' who he maintained contact with via a regular newsletter and C's being archived customers.	

10.3.6 Training

Examples of good practice	Examples of poor practice
• A GI Intermediary used an on-line training website (costing around £100 per employee per year). The firm believed that the training was good quality and included separate modules on financial crime which were compulsory for staff to complete. Staff were also required to complete refresher training. An audit of all training completed was stored on-line.	• A GI Intermediary explained that the compliance manager carried out regular audits to confirm staff knowledge was sufficient. However, on inspection of the training files it appeared that training was largely limited to product information and customer service and did not sufficiently cover financial crime.
• An IFA (sole trader) carried out on-line training on various financial crime topics. He also participated in conference call training where	• One credit union, apart from on-the-job training for new staff members, had no regular training in place and no method to

a trainer talked trainees through various topics while on-line; this was both time and travel efficient.	test staff knowledge of financial crime issues.

10.3.7 Responsibilities and risk assessments

Examples of good practice	Examples of poor practice
• At an IFA there was a clearly documented policy on data security which staff were tested on annually. The policy contained, but was not limited to, details around clear desks, non-sharing of passwords, the discouraging of the over-use of portable media devices, the secure disposal of data, and the logging of customer files removed and returned to the office.	• At an IFA, a risk assessment had been undertaken by the firm's compliance consultant but the firm demonstrated no real appreciation of the financial crime risks in its business. The risk assessment was not tailored to the risks inherent in that business.
• An IFA had produced a written data security review of its business which had been prompted by their external consultants and largely followed the small firms' factsheet material on data security, provided by the *FSA* in April 2008.	• An advising-only intermediary had its policies and procedures drawn up by an external consultant but these had not been tailored to the firm's business. The MLRO was unclear about investigating and reporting suspicious activity to SOCA. The firm's staff had not received formal training in AML or reporting suspicious activity to SOCA.
• In a personal pension operator, there was a full and comprehensive anti-fraud strategy in place and a full risk assessment had been carried out which was regularly reviewed. The firm's financial transactions were normally 'four eyed' as a minimum and there were strict mandates on cheque signatures for Finance Director and Finance Manager.	

10.3.8 Access to systems

Examples of good practice	Examples of poor practice
• In a Discretionary Investment Management firm, the Chief Executive ensured that he signed off on all data user profiles	• In a financial advisory firm there was no minimum length for passwords, (although these had to be alpha/numeric) and the prin-

ensuring that systems accesses were authorised by him.	cipal of the firm plus one other colleague knew all staff members' passwords.
• A discretionary investment manager conducted five year referencing on new staff, verified personal addresses and obtained character references from acquaintances not selected by the candidate. They also carried out annual credit checks, CRB checks and open source Internet searches on staff. There were role profiles for each job within the firm and these were reviewed monthly for accuracy.	• In an advising-only intermediary, staff set their own systems passwords which had no defined length or complexity and were only changed every six months.
• In a venture capital firm they imposed a minimum ten character (alpha/numeric, upper/lower case) password for systems access which had a 45-day enforced change period.	

10

10.3.9 Outsourcing

Examples of good practice	Examples of poor practice
• A discretionary investment manager used an external firm for IT support and had conducted its own on-site review of the IT firm's security arrangements. The same firm also insisted on CRB checks for cleaners.	• An authorised professional firm employed the services of third-party cleaners, security staff, and an offsite confidential waste company, but had carried out no due diligence on any of these parties.
• An IFA had received a request from an introducer to provide names of customers who had bought a certain financial product. The firm refused to provide the data as it considered the request unnecessary and wanted to protect its customer data. It also referred the matter to the Information Commissioner who supported the firm's actions.	• An IFA allowed a third-party IT consultant full access rights to its customer databank. Although the firm had a service agreement in place that allowed full audit rights between the advisor and the IT company to monitor the security arrangements put in place by the IT company, this had not been invoked by the IFA, in contrast to other firms visited where such audits had been undertaken.
• A general insurance intermediary employed office cleaners supplied by an agency that conducts due	• In an authorised professional firm, Internet and Hotmail usage was only monitored if it was for

diligence including CRB checks. Office door codes were regularly changed and always if there was a change in staff.	longer than 20 minutes at any one time. There was also no clear-desk policy within the firm.
• In an authorised professional firm, unauthorised data access attempts by staff were monitored by the IT manager and email alerts sent to staff and management when identified.	• In an authorised professional firm there had been two incidents where people had walked into the office and stolen staff wallets and laptops.
• In a general insurance intermediary the two directors had recently visited the offsite data storage facility to satisfy themselves about the security arrangements at the premises.	

10.3.10 Physical controls

Examples of good practice	Examples of poor practice
• At an IFA, staff email was monitored and monthly MI was produced, which included a monitoring of where emails had been directed to staff home addresses.	• In a general insurance intermediary which had poor physical security in terms of shop front access, there were many insecure boxes of historical customer records dotted around the office in no apparent order. The firm had no control record of what was stored in the boxes, saying only that they were no longer needed for the business.
• At an investment advisory firm, staff were prohibited from using the Internet and Hotmail accounts. USB ports had been disabled on hardware and laptops were encrypted.	

10.3.11 Data disposal

Examples of good practice	Examples of poor practice
• An advising and arranging intermediary used a third party company for all paper disposals, using secure locked bins provided by the third party. All paper in the firm was treated as confidential and 'secure paper management' was encour-	• In an IFA there was a clear-desk policy that was not enforced and customer data was stored in unlocked cabinets which were situated in a part of the office accessible to all visitors to the firm.

	aged throughout the firm, enhanced by a monitored clear-desk policy. The firm was also aware that it needed to consider a process for secure disposal of electronic media as it was due to undergo a systems refit in the near future.
• An IFA treated all customer paperwork as confidential and had onsite shredding facilities. For bulk shredding the firm used a third party who provided bags and tags for labelling sensitive waste for removal, and this was collected and signed for by the third party. The firm's directors had visited the third party's premises and satisfied themselves of their processes. The directors periodically checked office bins for confidential waste being mishandled. PCs which had come to 'end of life' were wiped using reputable software and physically destroyed.	

10

10.3.12 Data compromise incidents

Examples of good practice	Examples of poor practice
• A general insurance broker had suffered a succession of break-ins to their offices. No data had been lost or stolen but the firm sought the advice of local police over the incidents and employed additional physical security as a result.	• In a general insurance intermediary, the IT manager said he would take responsibility for any data security incidents although there was no procedures in place for how to handle such occurrences. When asked about data security, the compliance officer was unable to articulate the financial crime risks that lax data security processes posed to the firm and said it would be something he would discuss with his IT manager.

10.3.13 General fraud

Examples of good practice	Examples of poor practice

- A small product provider had assessed the fraud risk presented by each product and developed appropriate controls to mitigate this risk based on the assessment. This assessment was then set out in the firm's Compliance Manual and was updated when new information became available.
- A credit union did not permit its members to change address details over the telephone. These needed to be submitted in writing/email. The firm also considered the feasibility of allocating passwords to their members for accessing their accounts. The union had photographs of all its members which were taken when the account was opened. These were then used to verify the identity of the customer should they wish to withdraw money or apply for a loan from the union.
- One discretionary investment manager kept full records of all customer contact including details of any phone calls. When receiving incoming calls from product providers, the firm required the caller to verify where they were calling from and provide a contact telephone number which they were then called back on before any customer details were discussed or instructions taken.
- One general insurance intermediary was a member of a local association whose membership included law enforcement and Law Society representatives. This group met in order to share local intelligence to help improve their firms' de-
- One GI broker permitted customers to contact the firm by telephone to inform the firm of any amendments to their personal details (including change of address). To verify the identity of the person they were speaking to, the firm asked security questions. However, all the information that the firm used to verify the customer's identity was available in the public domain.

	fences against financial crime.

10.3.14 Insurance fraud

Examples of good practice	Examples of poor practice
• A small general insurer had compiled a handbook which detailed indicators of potential insurance fraud.	• An IFA had a procedure in place to aid in the identification of high risk customers. However, once identified, this firm had no enhanced due diligence procedures in place to deal with such customers.
• An IFA had undertaken a risk assessment to understand where his business was vulnerable to insurance fraud.	
• An IFA had identified where their business may be used to facilitate insurance fraud and implemented more controls in these areas.	

10.3.15 Investment fraud

Examples of good practice	Examples of poor practice
• An IFA had undertaken a risk assessment for all high net worth customers.	• An IFA had a 'one size fits all' approach to identifying the risks associated with customers and investments.
• A discretionary investment manager referred higher risk decisions (in respect of a high risk customer/value of funds involved) to a specific senior manager.	
• A personal pension operator carried out a financial crime risk assessment for newly introduced investment products.	

10.3.16 Mortgage fraud

Examples of good practice	Examples of poor practice
• The majority of firms conducted customer fact finds. This allowed them to know their customers sufficiently to identify any suspicious behaviour. CDD (Customer Due Dili-	• An IFA did not undertake any KYC checks, considering this to be the responsibility of the lender.

gence. See FCG Annex 1 for common terms), including source of funds information, was also obtained early in the application process before the application was completed and submitted to the lender.	
• A home finance broker would not conduct any remote business – meeting all customers face-to-face.	• An IFA did not investigate source of funds. The firm stated this was because 'a bank would pick it up and report it.'
• An IFA had informally assessed the mortgage fraud risks the business faced and was aware of potentially suspicious indicators. The IFA also looked at the fraud risks associated with how the company approached the firm – e.g. the firm felt that a cold call from a customer may pose a greater risk than those which had been referred by longstanding customers.	• An IFA did not undertake extra verification of its non face-to-face customers.

10

10.3.17 Staff/Internal fraud

Examples of good practice	Examples of poor practice
• An IFA obtained full reference checks (proof of identity, eligibility to work and credit checks) prior to appointment. Original certificates or other original documentation was also requested.	• One general insurance intermediary did not undertake any background checks before appointing a member of staff or authenticate qualifications or references.
• An IFA ensured that staff vetting is repeated by completing a credit reference check on each member of staff.	• Company credit card usage was not monitored or reconciled at an IFA. An IFA had the same computer log-on used by all staff in the office no matter what their role.
• An IFA set a low credit limit for each of its company credit cards. Bills are sent to the firm and each month the holder has to produce receipts to reconcile their claim.	
• At one authorised professional firm dual signatory requirements had to be	

	met for all payments made over £5,000.