

## **Boiler Room Operations - Financial Services Watchdog and the City of London Police join forces.**

**(First published under 'City Comment', in The Company Lawyer, Vol 31, No 5, 148-9, May 2010)**

In a recent press release, the Financial Services Authority (FSA) stated that together with the City of London Police it had written to 6,500 homes across the UK to warn people that their details are on a 'Master list being used by share fraudsters to target people and sell them worthless shares. The list contains the names of about 10,000 people, some with addresses and phone numbers. The list was discovered by the FSA and City of London Police who launched a joint operation aptly called Operation WARN. The letter, which is the first stage of operation WARN, explains what people on the list can do to protect themselves from the fraud.

### **Techniques employed by a boiler room operation.**

There are numerous techniques that are employed by such operations to contact members of the public. For example, some victims of boiler room fraud have commented that they were contacted 'out of the blue' on the telephone while other victims were contacted by marketing firms working on their behalf. A typical scenario is that a boiler room will approach a small company in the UK and propose to raise capital by selling £100,000 to £200,000 worth of shares in that same company on their behalf. Of this amount, for example £100,000, the boiler room would take 60 percent or higher as their fee, leaving the small company with £40,000 capital. In reality, the boiler room will cold call UK investors to sell the shares at anything from 10 to 100 percent over and above the agreed price, take their fee and vanish. Investors are directly affected by such scams, because they are being enticed to pay over the odds for the shares. The UK Company also suffers, as its shares are being sold by a boiler room, leaving it exposed to potential financial losses and/or damage to its reputation. If the boiler room is taking a large percentage of the funds raised, many small companies would struggle to refund investors with the full price that was paid for the share.

### **Who exactly are the victims of this fraud?**

There is not a stereotyped victim of this financial crime, notwithstanding the portrayal in the press of elderly or retired victims that have succumbed to investing in non-existent financial products. On the contrary, other victims include experienced investors such as lawyers, accountants and bankers who have equally been defrauded by these criminal entities.

For example, in 2004, the FSA conducted a survey of the 105 people who had telephoned its consumer helpline because they had fallen victim to investment scams orchestrated by boiler room operations. The FSA's research discovered that the majority of victims were male; most callers were aged between 35-55. However, a large percentage of calls had been made by people who were over the age of 55 years old or retired. Interestingly, the callers were from a variety of backgrounds, but 30% were professionals or directors. Of particular interest to the FSA, their research indicated that boiler rooms would target elderly members of the public. Of those who had fallen victim to boiler rooms, 38% were aged over

60 years old, while 26% of victims were 51 to 60 years old, the majority of victims were male 81% and most were experienced investors, with 41% of victims stating that they had been investing for over 11 years.

Further to this survey, the FSA in 2006 carried out further research, to demonstrate how boiler rooms operate, as part of its campaign to raise awareness of this financial crime. The results of the survey identified that the members of the public who had fallen victim by purchasing worthless shares lose an average £20,000. 58% of the respondents to the survey had fallen victim to boiler room fraud, of the 58% of those victims, 13% had been conned by more than one boiler room, while 3 victims each had reported losses of over £100,000.

Despite these renewed efforts by the FSA and the City of London Police, it is important to note that share fraud is not a recent phenomenon.

### **The need to raise awareness**

Yet ask people if they know what is a boiler room scam and most, regardless of whether they are professional people, serious investors, elderly people, or ordinary employees, are hard pressed to define or describe it. Raising awareness of the threat of boiler room scams has, therefore, to be a key weapon in the fight to reduce their number and impact. But by and large, training provided by UK firms is targeted at specialists; those who operate in fraud detection, investigation, risk, compliance, audit, and accounting; those very people who know what boiler room scams are and who are least likely to need their awareness raising. The result is that real knowledge of how this financial crime is committed and how one might protect oneself from it, remains in the heads of the very few, whilst increasingly, the evidence referred to above, indicates that the victims are drawn from all walks of life.

So how can training be better targeted and better tailored so that the risk of financial crime such as boiler room scams be minimised?

First, it is important to recognise that what makes boiler room scams succeed is information; typically personal information. This is the personal information that fraudsters collect:

- legitimately, or otherwise, about their potential targets, including their names, dates of birth, contact details, share ownerships, propensity to invest, etc;
- about the companies they target and on whose behalf they purport to sell shares;
- that individuals unwittingly provide about themselves as they fall victims to these scams and that are subsequently used again by fraudsters to defraud their victims again and again.

Take Jean, for example. Jean received a 'phonecall ostensibly from her insurance company, apparently in response to a letter she had previously written them. The caller announced his name, the reason he was calling and asked Jean to confirm her postcode, date of birth and mother's maiden name so that he could verify her identity. Willingly she confirmed all of these. What is it that makes us so willingly and without the hint of suspicion, hand over personal information to people we have never previously met, yet who sound, convincingly, as if they have some official and legitimate reason for having it? When we behave like this willingly in our private lives, our behaviour spills over into our working lives, which leaves us not only individually vulnerable, but also puts our businesses at risk.

Many agencies are now talking of raising awareness in order to combat financial crime. As financial crime increases, so too, does the need to raise public awareness. But what we so often forget is that our own employees are not just employees of our organisations; they are members of the general public too. If firms raise their employees' general awareness of financial crime, not only do they help the general public protect themselves, they help protect their employers too.

So what can UK firms do to raise awareness of boiler room scams and other financial crime, so minimising risk to their businesses, their customers and to their employees? They can

- target all their employees, rather than just specialists, so that everyone knows what are boiler room scams, how they can protect themselves from falling prey and how they can protect UK businesses;
- demonstrate the connection between information security, financial crime and data protection, (so many training programmes artificially compartmentalise these areas and so fail to convey that financial crime is often the result of a failure to maintain robust personal or organisational information security); and
- bring information security, financial crime and data protection to life for ordinary people in a way that captures their imaginations, changes their attitudes and behaviours and makes them less willing to divulge information, whether that is their own, their customers' or sensitive company information.