Crime and Corruption Commission
QUEENSLAND

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

ASIC
Australian Securities & Investments Commission

July 2016

Cold-call investment fraud

How organised crime is targeting your money

Cold-call investment fraud generally starts with a phone call that offers the opportunity to be part of a lucrative investment. In most cases, it ends with the company shutting up shop, only to re-emerge somewhere else under another name, looking for new prospective clients. And the investor? In most cases they lose all the money they put into the venture, with no means of recouping their losses.

Make no mistake – cold-call fraud is organised crime, costing Australians millions of dollars each year. But it can be stopped if people just hang up the phone.

What you should know

- Historically cold-call investment fraud had been committed by criminal networks operating from overseas, mostly Asia, but this type of crime is now being set up and operated from within Australia.
- Cold-call investment fraud is a complex crime type involving criminal, consumer and corporate law, making it difficult to pursue and prosecute.
- The main targets for this type of fraud are middle-aged and older Australians with good jobs or recently retired.
- As criminal groups quickly withdraw the funds in cash or transfer the money offshore, you are unlikely to get your money back.
- Investor or public awareness is the best response to this type of fraud – an informed public can recognise the signs of criminal intent behind a seemingly legitimate investment offer.
- Cold-call investment fraud is one crime type in which prevention is undoubtedly better than cure.

The information contained has been provided by the Crime and Corruption Commission, Queensland Police Service, Australian Criminal Intelligence Commission and Australian Securities & Investments Commission to inform the public about serious and organised crime.

What is a cold-call investment fraud?

Cold-call investment fraud, also known as boiler room fraud, is a type of organised crime in which a group of criminals set up an elaborate façade of legitimate business to defraud people by getting them to invest in opportunities and companies that do not deliver as promised.

The fraud involves a person receiving an unsolicited contact, usually a telephone call out of the blue (a cold call) or an email, connecting them with a salesperson. The salesperson builds rapport with the investor, using various techniques designed to induce the person to invest in what is claimed to be a highly profitable money-making venture. The investment opportunity is of course fraudulent and there is no possibility that it will ever deliver the promised results. Once the criminal group has obtained money from a number of investors, they shut down the particular company, with the investor often losing all the money they handed over.

Criminals running cold-call fraud have been targeting Australian investors since the 1990s, through schemes set up either overseas or within Australia.

The cost of cold-call fraud

The total cost of cold-call fraud to date is difficult to measure accurately, but it can be counted in both the financial loss and the personal impact on those who invested their money in such schemes.

Financial cost

A recent operation by the Crime and Corruption Commission (CCC) and the Queensland Police Service (QPS) (Operation Sterling) has focused on 11 networks believed to have been involved in cold-call fraud on the Gold Coast and in Brisbane. It has been conservatively assessed that cold-call fraud originating *only* from these 11 networks cost the Australian public at least $30 million a year. Judging by the latest Australian Competition and Consumer Commission report, investment fraud originating from overseas has been reported as costing the Australian victims $24 million in 2015, bringing the total potential annual loss in Australia from cold-call fraud to over $50 million a year. This is a highly conservative estimate, and the real loss almost certainly exceeds this figure multiple times.

The true dollar cost of this fraud type is also hard to measure due to significant under-reporting. Only one in four investment fraud victims, who had lost between $1000 and $25 000, admitted to being scammed.[1] Some of the reasons for not reporting included investor uncertainty as to whether they had been involved in an actual fraud or simply a bad investment, a lack of definite evidence or not knowing who to report their case to.[2]

Who is targeted?

Victims can be anyone but tend to be middle-aged to older Australians, including recent retirees, educated, computer-literate and on a higher income.

Australians are a key target group of investment fraud because:

- they are a receptive audience to offers to “invest”;
- Australia is a relatively wealthy country where people have funds to invest; and
- there is unprecedented interest in the investment market by retail investors.

With the cost of fraud so high, and its impact so potentially devastating, it is vital that people know how to see through the scams — to recognise the signs and tactics of criminal activity behind seemingly legitimate offers.

1 AARP, 2003

2 *Scams, schemes & swindles, A review of consumer financial fraud research 2012*, fraudresearchcenter.org (accessed 29 May 2016)

How organised crime groups create a fraud

The conversation that begins when a person picks up the phone is in fact a calculated step in a highly planned criminal operation, designed with two things in mind:

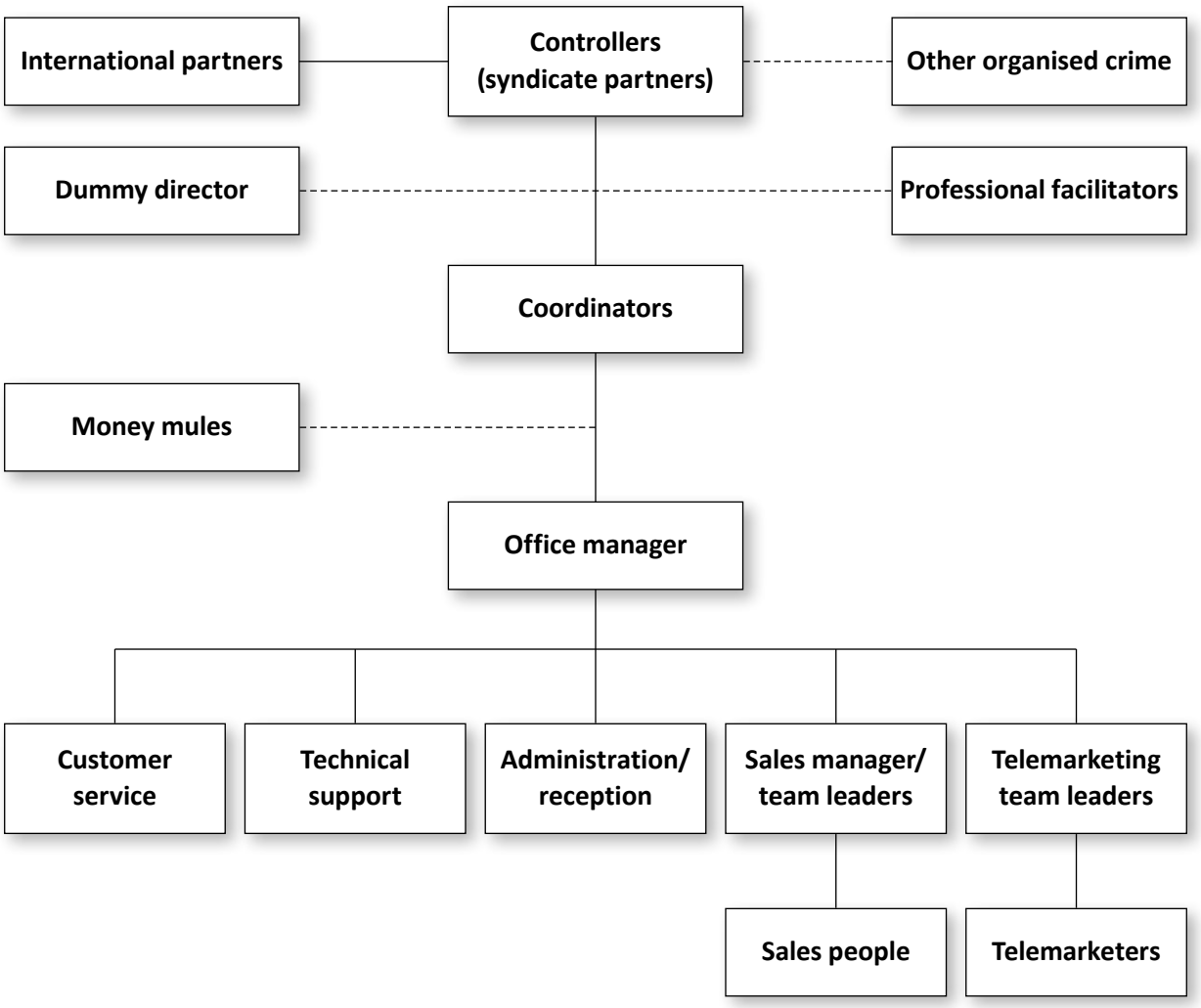
- To rob potential investors of their money, using the pretence of a legitimate and lucrative business opportunity, and
- To make detection and investigation of the fraud difficult, and recovery of the invested funds almost impossible.

The fraud methodology described below comes from recent investigations and intelligence hearings undertaken by the CCC and the QPS as part of Operation Sterling [see case study on page 6].

1. Putting a team together

Each cold-call investment scheme requires a range of skills and capabilities that will each play a part in executing the fraud. These include managers, sales staff, customer-service staff, professional facilitators to set up companies, IT developers, telemarketers, compliance staff, lead suppliers, money mules, dummy directors, and bookkeepers or accounts payable staff. The figure below depicts the staff structure of a typical cold-call fraud operation.

Cold-call investment fraud organisation structure



The operators of these schemes have a strong focus on developing and motivating staff with the skills they need to be convincing and to insulate the scheme from adverse attention for as long as possible. Management and sales staff have often worked across the operations of multiple syndicates. Staff are trained using films such as *The Wolf of Wall Street* and provided with incentives such as generous commission schemes and overseas trips. There is a strong focus on the use of professional sales techniques and high-pressure sales psychology designed to create in the target investor a sense of urgency and obligation to invest.

2. Behind the scenes: how they make it look real

Cold-call fraud operators put significant effort into making sure that the scheme appears professional and legitimate, taking care to conceal the fraudulent activities and the identities of key participants.

The vehicle for Australian-based schemes is a company, registered either in Australia or in a foreign country, often a nation with lax regulatory standards. Having a registered company contributes to the perception of legitimacy. The principal beneficiaries of the scheme usually use "dummy" directors to conceal their links to the company.

Cold-call fraud companies market and sell "money-making or investment opportunities" – products or services that are claimed to provide financial returns well in excess of market averages. The products or services align with a legitimate commercial industry such as horse racing, sports betting, financial markets "trading" in the stock market or foreign exchange markets, or a derivative market such as index or binary options trading.[3] The products or services range from provision of racing tipping services to "predictive" software programs which facilitate trading. However, "trading" does not mean the usual types of trading in markets – purchases and sales of stocks, currencies or commodities. Instead it means placing bets such as gambling on market movements (up or down). In fact, whatever the supposed trading activities, typically they are fictitious and there are no trades made.

"Reputation managers" (who may be drawn from any level of the structure) are engaged to post fake positive reviews of products on the internet. Should an investor seek to undertake due diligence on the company or product, the reputation managers ensure that any adverse references are pushed down the order of appearance in search results.

Cold-call fraud networks change their company names frequently and new or rebranded products are developed. This allows the operators of the scam to further distance a new or "phoenixed" company from adverse reporting on a previous company or product.

Once the various fraudulent companies, products and services, and team members are in place, the cold-calling begins.

3 Forms of betting on the upward or downward movement of a stock on the market

3. Engaging potential investors: the cold-calling process

Step 1

The marketing and sales process starts with telemarketing staff cold-calling people to interest them in the idea of a money-making investment opportunity and set them up for a follow-up contact from a salesperson. The telemarketers are given contact details for the people (referred to as the "leads") they cold-call. Names and details are on leads lists or databases obtained by the company from one or more sources, legally or otherwise.

Step 2

Once a person has indicated some interest in the opportunity (and are now referred to as "qualified leads"), they are passed from the telemarketing call centre to the sales office. Using an established script, the salesperson calls the "qualified lead" and uses sales techniques to persuade them to enter into a contract to invest money in the company's product or service. The salesperson identifies and explores the person's desires or fears to focus attention on the profits to be made, and keeps the description of the product as brief as possible. Prepared rebuttals are used to counter any concerns or objections raised. Repeated calls to the person are often made.

Step 3

Potential clients may be referred to the company's website and offered online demonstrations of the product, conducted using the website. The high-quality appearance and apparent functionality of the website often impress and help to convince potential clients of the legitimacy of the company and the viability of the products or services it offers. Should a person resist these efforts they may be passed to a more senior representative of the company to assist in completing the sale.

Step 4

Products are often sold in price-point structured packages and, though not initially revealed by the sales person, significant discounts may be available on each package depending on the potential buyer's financial circumstances. Once the new "client" signs a contract worth between $5000 and $50 000, they may be referred to "customer service" or "technical support". Customer-service staff provide assistance to the client, for example with operating the software, and also deal with any later concerns or complaints, often by referring the client to the detail in the contract's "fine print".

Step 5

Soon after the buyer's funds are transferred to the company bank account, they are usually withdrawn or transferred to another bank account controlled by the parent syndicate. Looking at their trading account on the company website, buyers may see their investment appear to be growing, but in reality the victim can no longer access their own money. At a later date victims may be offered, for a much larger investment, an "upgraded" product or service with promises of even greater returns. This upgrade is fictitious, generating no returns for the victim but substantial profits to the syndicate.

Step 6

When the income generated through the sale of the fraudulent products or services falls near to or below the operational costs of the cold-call fraud, the company "phoenixes". This usually occurs due to bad publicity about the company, either on the internet or by word of mouth, significantly reducing the available pool of potential victims. Professional facilitators are then used to register a new company, the products or services are rebranded, the call centre may relocate, and the next cycle of the scam begins.

The following case study from Queensland illustrates the organised crime frameworks and linkages behind the scams themselves.

Case study

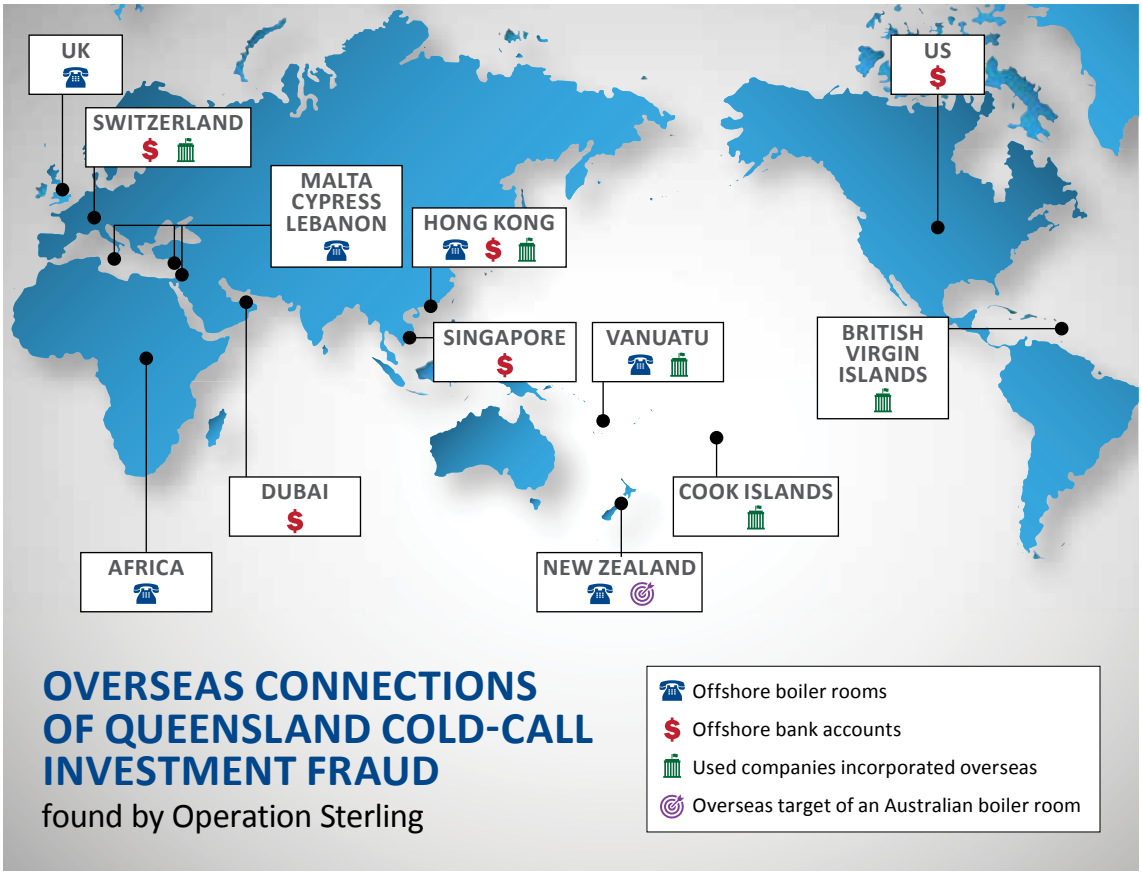
Cold-call fraud in Queensland: Operation Sterling

In 2016 the CCC and the QPS commenced Operation Sterling to gather intelligence on the activities of 11 cold-call fraud operations and criminal organisations that have operated on the Gold Coast, in Brisbane and overseas.

The 11 networks examined were active in Australia between 1994 and the present day. It is estimated that more than 113 separate fraudulent schemes have been conducted in Queensland by these syndicates during this time — not including schemes controlled by these syndicates and located offshore.

Overseas connections

Eight out of the 11 cold-call investment fraud syndicates examined had significant overseas connections, as illustrated below.



Links to traditional organised crime

Operation Sterling revealed well established links between cold-call investment fraud operations and traditional organised crime. It is believed that some cold-call operations are controlled and coordinated by criminal entities linked to outlaw motorcycle gangs (OMCGs) and other established organised crime syndicates.

Five out of the 11 syndicates have been identified as having direct links with established traditional Australian organised crime identities or OMCGs also involved with the importation and distribution of illicit drugs. Money obtained through cold-call fraud is also being used to fund loan-sharking and other organised crime activities.

Taking action against cold-call fraud

Cold-call investment fraud is a complex crime type involving criminal, consumer and corporate law, making it difficult to pursue and prosecute. Law enforcement agencies, financial regulators and other bodies have all worked both independently and collaboratively across Australia to tackle the problem.

Networks can rapidly "phoenix" from one company to another in order to minimise real-time detection. Penetrating the veneer of legitimacy and multiple layers of bank accounts, dummy directors and investment opportunities requires protracted investigation and expert forensic financial analysis to gather evidence for any court action to be taken.

The fraud often involves multiple complainants across multiple jurisdictions, and the cold-call methodology ensures that suspicions or complaints are delayed until such time as the offending company no longer exists. This most often means that law enforcement has to focus on historical investigations being conducted after both monies and fraud operators have gone.

Once investors' money has been disbursed there are no effective and timely proceeds of crime or civil remedies for authorities or individual investors to recover the funds.

Cold-call investment fraud is one crime type in which prevention is undoubtedly better than cure.

Common warning signs

The common warning signs of cold-call investment fraud are:

- An "out of the blue" (random or unexpected) contact
- A "too good to be true" offer of unrealistic (high) returns or profits
- A 1300 or 1800 number used
- Use of financial terms e.g. "trading", "investment", "tax-free", "low-risk", "risk-free profit"
- A virtual address or serviced office used, for example, serviced office operated by Servcorp.

To protect yourself you can:

Hang up on unsolicited telephone calls offering investments.

Visit www.moneysmart.gov.au or call **1300 300 630** for more information or advice.

Alert your family and friends to these investment frauds, especially those who may have savings to invest.

Report suspected investment frauds to the Australian Securities & Investments Commission, through **www.moneysmart.gov.au** or **1300 300 630**, the Australian Competition and Consumer Commission through **www.scamwatch.gov.au**, or your local police. *Any information that can be provided such as company name, location and contact details will assist with subsequent investigations and enquiries.*

Check that any company you have discussed investments with has a valid Australian Financial Services Licence at **www.moneysmart.gov.au**.

Seek independent financial advice before making an investment.

Contact your financial institution immediately if you think you've been scammed to see whether they can retrieve funds invested or prevent further funds being lost.

AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION

www.ccc.qld.gov.au www.police.qld.gov.au www.acic.gov.au www.asic.gov.au