IFW

GLOBAL

A leading global cybercrime investigation agency

Online Investment Fraud

Recover Your Stolen Assets

IFWglobal.com

IFW

GLOBAL

IFW Global work in close alliance with international law enforcement agencies around the world to combat cybercrime and recover your stolen money.

CONTENTS:

Introduction	2
Types of investment fraud	3
How to spot an investment scam	5
How to recover stolen assets	6
Recovery Proceedings	7
Case studies of successful asset recovery	8
Where to get help	11
Contact IFW Global	12

5556448866650805686
10193642667390905601
14909171673811590019
87667355078439934693
81761792773562534671

> Losses to investment fraud in Australia increased by 33 percent in 2017 to $31.3 million.
>
> *– ACCC Targeting Scams report*

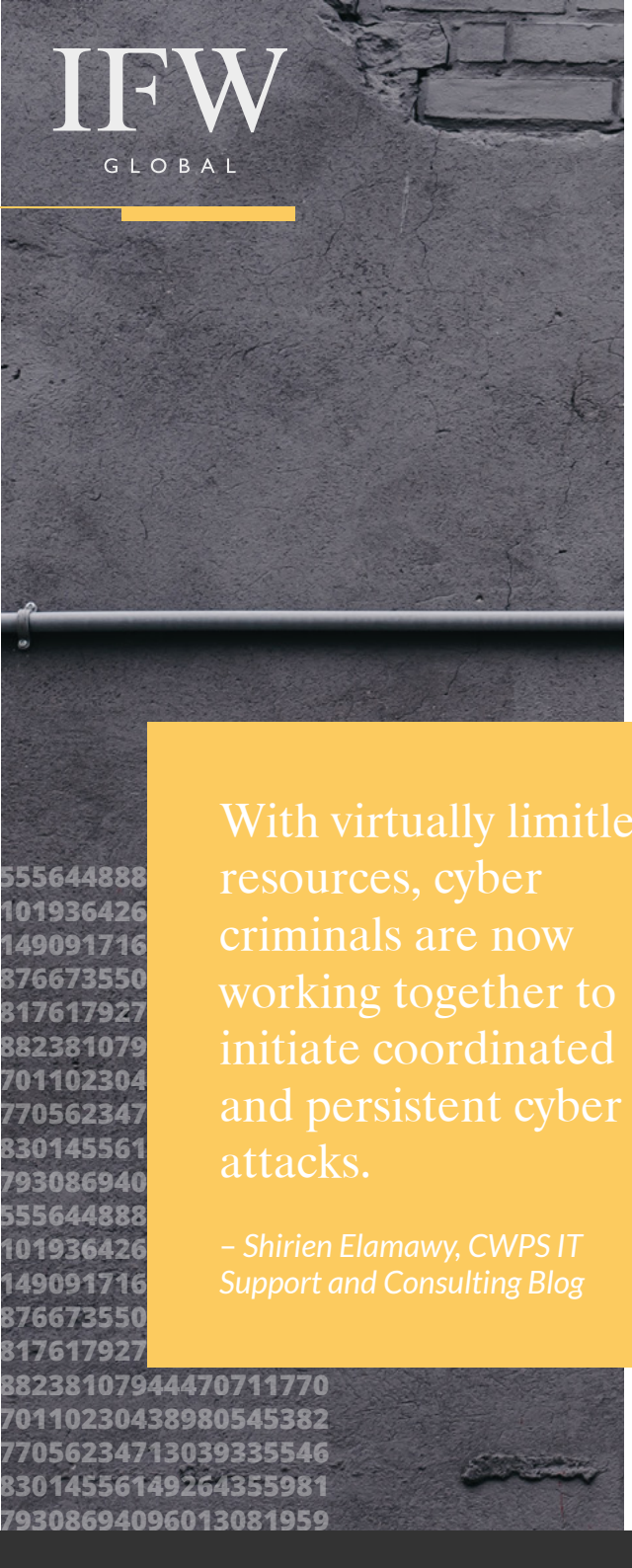
INTRODUCTION:

Do you believe you have lost money in an online trading scheme, online securities or investment fraud?

This is one of the fastest growing areas of white-collar crime in Australia and around the world. International criminal gangs have become increasingly adept at creating fictitious companies, websites, social media accounts and other materials that look legitimate, even to the trained eye.

Many hire experienced sales staff to work out of call centres ('boiler rooms') selling securities and investments such as blue-chip stocks or cryptocurrencies. They promise high returns for low risk. After they've gained your trust and you've invested an initial sum, they often use high-pressure tactics to get you to invest more, and make excuses about why you can't access your money.

Online investment fraud is perpetrated by professional criminals who target high-net-worth individuals and businesses. If you think you've been targeted by a cybercrime syndicate, a professional asset recovery and fraud investigation service could help recover stolen assets and bring the criminals to justice.



> With virtually limitless resources, cyber criminals are now working together to initiate coordinated and persistent cyber attacks.
>
> *– Shirien Elamawy, CWPS IT Support and Consulting Blog*

TYPES OF INVESTMENT FRAUD:

Cybercrime has become more sophisticated than simply spam emails which make exorbitant claims that are too good to be true. Professional criminal gangs have global operations and use a range of tactics to part investors from their hard-earned wealth. Below are some of the more common scams.

Cryptocurrency scams

The successes of Bitcoin and other online cryptocurrencies have provided a windfall for scammers. Using the same public funding model as many legitimate businesses, criminals posing as tech start-ups make an Initial Coin Offering (ICO) to investors, with the guarantee that their cryptocurrency will be valuable in the future. The fraudsters then disappear.

Binary options scams

A controversial type of speculative pricing investment, binary options offer 'all or nothing' outcome based on the performance of stocks or derivative investments (such as foreign exchange). Widely exploited by criminals, binary options fraud has resulted in US$10 billion in stolen assets each year, according to FBI estimates.

Sports trading scams

With the rise of prediction software and sports arbitrage, sports trading scams have become common over the past decade world-wide. The Australian Competition and Consumer Commission has warned against sports arbitrage schemes which guarantee profit from betting on all outcomes of a sporting event. In reality, investors are often defrauded.

Before making an investment online or over the phone, investors should always research thoroughly and consult with an asset recovery and fraud investigation service.

Private placement programs

Private placement programs (PPPs) can be legitimate trade platforms that are accessible only by invitation to high-net-worth investors. However, many of these platforms are really sophisticated fronts for criminal syndicates that demand high fees to gain access to their fraudulent trading platforms.

Advance fee scam

One of the best-known internet crimes, the advance fee scam or '419 scam', originated in Nigeria. It promises investors a share of a large fund or other asset if they provide an initial investment. If this payment is sent, the scammer will either end communication or make further excuses to extort more money.

Boiler room scam

A boiler room investment scam uses high pressure cold calling and dishonest sales tactics to sell a range of investments over the phone. Criminals promote purported stocks they have shares in, which drives up their value, so they can profit without returning anything to the investor. Boiler room scams are usually a cross-border crime, with call centres in the Philippines and other countries that use virtual offices to create the illusion of a large international financial advisory firm.

IFW
GLOBAL

HOW TO SPOT AN INVESTMENT SCAM:

Spotting online investment scams isn't always easy.

Criminal syndicates know that investors are likely to be suspicious of scams they have read or heard about. That's why many hire top web designers and graphic artists to make their websites, brochures and other materials look professional and legitimate. Well-spoken and experienced sales agents add to the image. Syndicates may even set up other fake organisations such as escrow companies and law firms to support the scam and make their claims more convincing.

However, there are often tell-tale signs with fraudsters. They include:

- receiving an offer by email, social media, pop up advertisement or cold call by phone
- the organisation has no financial services (AFS) licence in their country of jurisdiction
- it is based overseas often, in Asia
- you are contacted repeatedly
- callers insist that you act now.

Never invest your money until you have researched a company thoroughly.
If in doubt, contact a cybercrime agency.

> Investment scams cost Australians more than $26 million in the first six months of 2018 alone.
>
> *– ACCC Scamwatch*

HOW TO RECOVER STOLEN ASSETS:

If you've invested money and there are delays receiving your expected payment, the company is no longer replying, or you must pay additional fees to access your funds, it's unlikely you'll get your money back by waiting.

As most investment fraud involves cross-border crime, you cannot rely on local law enforcement agencies. In these situations, consider reaching out to a lawyer or asset recovery service for some options.

Recovering stolen assets is not always possible. Legal fees, court fees, investigative services and other expenses can be costly, especially in cross-border crime cases. Asset recovery services may be too expensive for recovering small amounts but for more serious fraud cases, the investment can be justified.

> Talk to your lawyer or a fraud investigation service about whether asset recovery is likely to be successful in your circumstances.

IFW
GLOBAL

RECOVERY PROCEEDINGS:

The first step in any asset recovery is to alert the bank which has received your money.
While the bank may decide to freeze the account, if it suspects unlawful activity has occurred, this alone won't help recover your money. Legal action must be taken in the jurisdiction where the bank is located, whether in Australia or overseas.

Cross-border crime

Investment fraud targeting investors typically originates in an overseas region where online criminal syndicates face little action from law enforcement. It can also take place across multiple regions in a deliberate effort to make investigation and fraud recovery more complex. Asset recovery in these situations requires the use of an experienced cybercrime agency that is familiar with local laws in multiple jurisdictions and is capable of obtaining the hard evidence needed.

How IFW Global can help

IFW Global is an international private intelligence and cybercrime investigation firm that has recovered millions of dollars in investment fraud and other internet crimes for clients.
Our experienced investigators can track down stolen funds, freeze bank accounts and initiate legal proceedings against suspects, leading to prosecution or private settlement in many cases.

THREE CASES OF SUCCESSFUL ASSET RECOVERY:

These case studies show how IFW Global investigators helped individuals and businesses recover stolen assets by identifying, exposing and disrupting financially-motivated criminals and syndicates in Australia and overseas.

Case study 1: sports trading scam – AUD $8.5 million recovered

IFW was hired to locate Peter Foster, a convicted fraudster wanted in Australia after failing to appear in the Federal court. Within three weeks IFW had tracked Mr Foster down. He was jailed for a year for contempt of court.

During his arrest, it emerged that Mr Foster was the mastermind behind a sports trading scam operating from his home between 2012 and 2014. This online scam promised lucrative returns to investors who paid for exclusive access to sport prediction software and savants.

A number of investors contacted IFW to help recover their stolen assets and a class action lawsuit was filed in Australia. Other actions taken by IFW in foreign jurisdictions led to the discovery of bank accounts owned by associates of Mr Foster in Vanuatu, the Cayman Islands and Hong Kong.

IFW orchestrated the freezing of all offshore bank accounts and the stolen assets were recovered. Mr Foster was arrested and charged with criminal offences related to the scheme.

IFW
GLOBAL

Case study 2: boiler room scam – USD $2.2 million recovered

IFW was retained to investigate Smith & Olsson, an organisation that claimed to be a leading financial advisory firm based in Philadelphia, USA. However, Smith & Olsson was identified as a boiler room investment scam operating out of the Philippines.

Sydney businessman, Mr A, had invested his life savings and superannuation of $1.8 million into the company, which used well-spoken brokers with English accents. The brokers were cold calling individuals and persuading them to invest in bogus stocks and shares. Mr A was coerced into paying taxes and other expenses in order to "cash out" his fund, and when he made demands to the broker handling his portfolio, the company closed down.

IFW tracked the boiler scam to the Philippines capital, Manila, and conducted an 18-month investigation. Eight arrest warrants were issued and the group's British mastermind was tracked, monitored and arrested in the Philippines in 2014. On his arrest, USD $2.2 million was discovered in two Hong Kong banks – in accounts under his name.

The accounts were frozen by IFW lawyers in Hong Kong. A Mareva injunction prevented any transfer of the funds. Facing serious charges, the fraudster negotiated a private settlement under which Mr A received USD $2.2 million on the withdrawal of his criminal complaint.

Case study 3: business loan fraud

Mr Y, the founder of a company that offered home loans, engaged IFW to find Mr Z, an Australian man who borrowed $170,000 on fraudulent terms.

Mr Z claimed his loan was used to buy high-end watches at a trade show for his jewellery business. Instead, he had used the loan to buy himself luxury goods. Confronted by Mr Y, he fled the country.

An arrest warrant was issued in Australia, but law enforcement agencies failed to locate Mr Z. IFW Global operatives traced the criminal to a coffee plantation in Indonesia, where he was arrested by Australian Federal Police.

Mr Z was served with a civil recovery claim and spent time in prison for the investment fraud.

IFW
GLOBAL

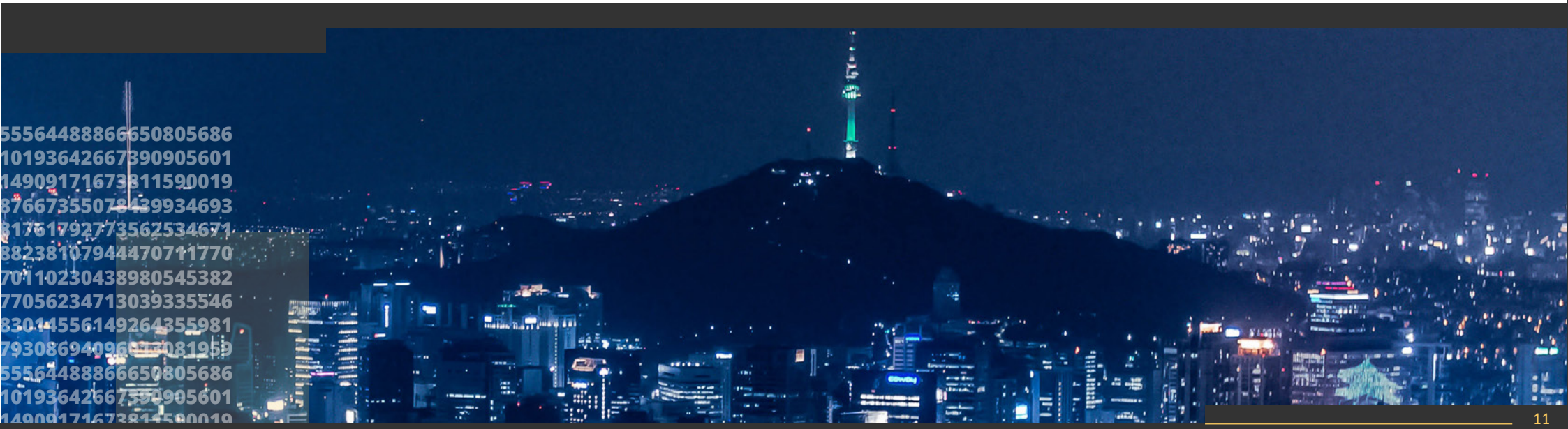
> It used to be the wealthier you were, the more immune you were to crime. Cyber crime has tipped it the other way.
>
> *– Neal O'Farrell, Executive Director, Identity Theft Council*

WHERE TO GET HELP:

Despite efforts by security services and law enforcement in Australia and around the world, investment fraud is a booming criminal industry that is expected to grow. Criminals are smarter and internet investment scams are evolving in sophistication. Without experience, it is sometimes almost impossible to determine which offers are authentic.

If you think you've lost funds to an online trading scam or investment fraud, IFW Global can help. Call us today on **(02) 9275 8725** to discuss your situation confidentially. Our cybercrime experts can advise whether fraud recovery is possible and how to bring the perpetrators to justice.

IFWglobal.com



IFW
GLOBAL

CONTACT IFW GLOBAL:

HEADQUARTERS

Level 32 BT Tower,
1 Market Street,
Sydney NSW 2000
Australia

P: +61 2 9275 8725
F: +61 2 9275 8800

Sydney | Manila | Bangkok
Hong Kong | London | Los Angeles