

## Notes

### ORGANIZED CRIME MAKES SWINDLING GO GLOBAL

**René Tapia**

[reneluis@iol.pt](mailto:reneluis@iol.pt)

Full He was born in Chile, and has Portuguese citizenship. PhD in Economics by the *Jules Verne University*, Amiens, France, and specialist in Drugs Political Economics. He has published extensively and been a speaker at several conferences in this field, and done research in offshore businesses and corruption. Professor at the Universities of the Algarve, Coimbra, and Lisbon, and his currently studying organized crime

*"L'argent apoudri".*  
Destanne De Bernis

In September 2007, EUROPOL and regulatory and consumer protection agencies in Australia, Belgium, Canada, the Netherlands, Nigeria, United Kingdom, and the U.S. created the International Mass Marketing Fraud Working Group (IMMFWG) with the aim of exchanging information and coordinating border operation to detect, apprehend and terminate mass marketing fraud, and improve public information on the international schemes operating in Africa, North America and Europe, as well as in Brazil, Costa Rica, United Arab Emirates, Philippines, Hong Kong, India, Israel and Thailand. This is an incisive global threat that affects millions of people and companies from around the world each year, representing losses of tens of billion dollars and the financial well-being of staff and families. In June 2010, the Group presented its report on "**Mass Marketing Fraud: A Threat Assessment**", on which this article is based.

Mass marketing fraud uses the Internet, mail, radio, television programmes, large concentrations of people or even "word of mouth" rumour; however, regardless of the means employed, it will always have the following two characteristics:

- 1) the scheme involves persuading a victim to transfer money or any valuable property to the criminal based on a promise of future profit or valuable services that the victim will never receive in practice;
- 2) the criminal command uses the scheme on many individuals or companies in order to maximize income.

The scheme resorts to a variety of tricks (pitches), such as lotteries, or winning tickets, investment opportunities, businesses involving counterfeit cheques, or "romance".



## Losses with mass marketing fraud

As most victims of mass marketing fraud do not complain, whether because they feel embarrassed or because they do not want to be involved in corruption schemes, there are no reliable statistics to assess the magnitude of this type of fraud on a global level. The British authorities estimate that only five per cent of people complain about fraudulent offers, and an investigation in Canada conducted in 2007 found that nine out of ten victims do not notify the authorities. However, other calculation methods suggest losses of about ten billion dollars per year.

The Office of Fair Trading in the UK in 2006 estimated that 3.2 million people (6.5% of adult population) were victims of the mass-marketing scheme, accounting for total losses of £3.5 billion. Similar studies, but not comparable, have been conducted in other countries, such as Australia, Belgium and the U.S., always exposing the deception of millions of people and involving millions of dollars (including foreign lottery schemes, “promotional prices” or Internet fraud)<sup>1</sup>.

However, fraud victims not only bear the financial costs or the loss of their savings and even homes, but also experience physical risks that can lead to depression or even suicide. Mere contact with the scheme may evolve to threats or kidnapping for ransom. However, there are records of cases when the family physically abused the kidnapped for having to pay a large sum for his/her release. Many people mortgage or sell their homes in order to enter the scheme or to pay back the debt, with subsequent loss of property. There is an additional serious economic consequence for legitimate trade and the institution of confidentiality of banking or commercial data: many victims of mass-marketing fraud change their behaviour with regard to shopping and their attitude towards purchases using credit cards, thus using them less, the same applying to online shopping.

## Pyramid investment scheme

Developed by mobster Carlo (Charles) Ponzi in the United States in the 1920s and lately by Bernard Madoff, or still “Dona Branca” in Portugal in the 1980s, it has been reinvented with the liberalization of Eastern European countries. It is a system that works in the short term with the first investors, but that ends up in bankruptcy for most unwary people involved in the scheme. It offers high yields at the expense of new investors and works as they increase exponentially, which is statistically unsustainable, as any basic mathematical calculation shows that a dozen iterations requires the participation of the entire world population. It consists of a payment or a payment promise of high interest rates at the expense of the money of the next investors. Several of these schemes have been uncovered lately, and in 2009 alone, just in the United States, they totalled \$16.5 billion. Ponzi started the business with \$5.000 and had deposits of 1 million when he was discovered six months later. Madoff was found

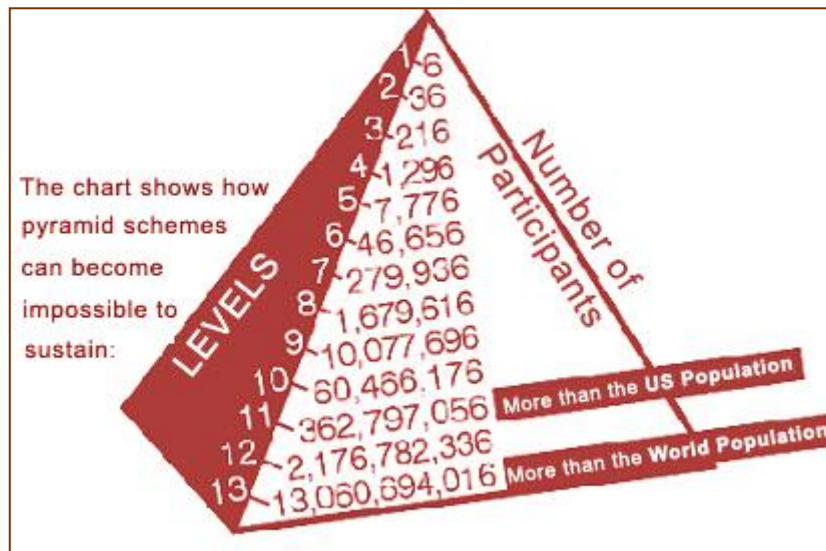
---

<sup>1</sup> The “Consumer Sentinel” network of the United States Federal Trade Commission (FTC) received 630.604 complaints in 2009, totalling US\$1.715.973.109, which is an average US\$2.721 per person. In the same year, the Canadian Anti-Fraud Centre reported over 40.000 complaints, totalling almost 60 million dollars, while in Australia there were over 20.000 complaints totalling 70 million dollars (The International Mass-Marketing Fraud Working Group, “Mass-Marketing Fraud: A Threat Assessment”, p. 5).



out as a result of the 2007 financial crisis and sentenced to 150 years in prison for fraud totalling \$65 billion<sup>2</sup>.

Maria Branca dos Santos started her activities in the late 1970s and when she was found out in 1984, she had raised 17.5 billion Escudos (\$130 million at the time)<sup>3</sup>.



Source: <http://upload.wikimedia.org/wikipedia/commons/2/2d/PyramidSchemeMS.jpg>

### Globalization of mass- marketing fraud

Although some crooks use fraud scams in their own localities, particularly the *Ponzi* scheme, recent investigations show that mass-marketing fraud schemes operate in a variety of countries in Africa, North, Central and South America, Asia, the Middle East, and in Europe, with a lot of similarities in their application, such as: choosing victims in different countries (we shall see further on that this fraud is dominated by international organized crime), internationalization of the laundering of the money obtained, hiring legal companies for carrying out the activities in preparation of the fraud (e.g., printing fake lotteries, conducting orders).

### Organized crime in action

This type of fraud can be conducted by an individual or a small group, varying in complexity and size according to its nature and structure. However, recent investigations have revealed that lately organized crime such as the U.S. *Cosa Nostra* or the Nigerian and Jamaican mafias lead or facilitate mass fraud scams, benefitting from their elaborate corporate structure<sup>4</sup>. Organized crime can control the entire

<sup>2</sup> <http://losangeles.fbi.gov/dojpressrel/pressrel10/la011210.htm>

<sup>3</sup> Since then the pyramid schemes offered by companies to potential consumers started to be considered to be "unfair trade practice" and legally prohibited (D.L. 57/2008).

<sup>4</sup> International organized crime, which is mixed with legitimate businesses, is involved in a wide variety of activities that are part of the economic cycle, including finance, major retailers, production, and transport. However, small trade or street distribution is left to "petty crime" or "street crime", which is controlled by



process or provide “specialized services” (false documents or websites, laundering, lists of people, financial instruments, etc.) running a comparatively lower risk of being detected or of facing potential penalty.

## The Process

Criminal investigation services have demonstrated the international nature of this fraud and of mafia rings in terms of their organization and control. They subcontract firms and employees to offer seemingly real products and services, and use sophisticated communication and processing technologies experienced in the diversion and concealment of goods and money. Victims are contacted by mail, via the Internet (the most used), radio and television, or in person; in most cases the request is initiated by telephone<sup>5</sup>.

## The means

This fraud requires a variety of means to find and communicate with the victim, as well as to obtain and legitimize illicit procedures and avoid being caught and investigated. First, the potential victim must be contacted, and then the procedures described above must be followed. This requires the following:

- 1) Legal business companies, which may or may not know the fraudulent nature of the business they are being hired for, or virtual companies, with or without a real address or telephone, which are necessary for printing, packaging, transporting, sending, or receiving false documents;
- 2) Mailing lists, which can be bought from other marketing companies, with names and contact details according to any organization criterion;
- 3) Payment procedures, often separated from the nature of the fraud to make it easier for the victim to re-collect the money (bank transfer, pre-dated cheques, credit card);
- 4) Communication methods and networks. The sophistication of this type of fraud requires access to an array of networked communication instruments: telephone cards, cell phones, internet cafes, email accounts, databases, and computerized data storage with enhanced features, etc., which make it difficult to identify the users. There are proven cases of transatlantic use of Internet or VoIP simulating a local call;

---

organized crime but conducted by small groups or gangs associated by a common characteristic: neighbourhood, ethnicity, etc. (R.T.).

<sup>5</sup> VoIP (Voiceover Internet Protocol) was created in 1974 by U.S. mathematicians, engineers in computer science with doctoral degrees in communication, Vinton Cerf, vice president of Google, and Robert Kahn, one of the creators of the Internet. It began to be developed in 2004 as mass marketing. It is the normal protocol used by any internet users, as this technology is used to receive written and spoken messages. The Voiceover Internet Protocol has many applications (free calls among some users, SMS messages, multimedia), but its technical nature makes it difficult to geographically locate users and it is susceptible of being violated. A “platform” of a company’s customers’ numbers can be sold to another company or be intercepted. As the voices are digitized and transmitted as a compressed “packet”, which the receiver plays as a stream, sophisticated technologies enable using a platform from abroad, simulating a local or national call to sell a product, offer a service or request humanitarian aid (R.T.).



- 5) False identity cards. They are absolutely necessary to open a bank account, install telephone services to contact the victims, pick up mail packages, and rent offices for enabling the fraud. Passports, identity cards, driving licenses, or work permits are tampered with when they are made or with regard to personal data, and many scammers have multiple identities, to the extent of one group of rogues having a common identity to obstruct the location of the crook and the interception of the network. Official documents such as cheques and others, both private and governmental, are also forged.
- 6) Method to avoid the police investigation of the fraud. Once the victim becomes aware of the fraud, the scammer changes method, using false names, often pretending to be the representative of prestigious organizations, and creating inaccurate email addresses. Some groups act by simultaneously making a counterfeit offer, and quickly changing the product when it is found out;
- 7) Identity theft and money laundering are the critical points of fraud schemes. The lists of potential customers may be bought or stolen from another company, and used for other purposes, to which the forgery of official companies can be added. Once they own the names and personal and financial information of customers, this can also be used fraudulently, simulating shopping or using the names without authorization, or even forging identity documents or violating databases. Once in possession of the money, scammers use formal or informal financial services, which can be legal or illegal, domestic or international and off shore, to transfer the money to its final destination.

All these procedures, such as the choice of victims, the origin of the money, beneficiaries, destination of the fraud, and methods are kept in great secrecy to prevent the authorities from both discovering the fraud and the amounts involved. For this reason, the requested forms of payment are cash, cheques, bank transfers, bank debit or credit card charging, varying according to the particular situation. Often the money changes hands and form until it reaches the final destination so as to hide personal enrichment and investment in new schemes. Some victims consciously continue to work with the criminals, in the hope of recovering some of the lost money<sup>6</sup>. It has not been demonstrated that the money is used to smuggle weapons or drugs.

### **Use of violence**

Swindling is a type of non-violent fraud, but some groups resort to coercive tactics in victims who do not cooperate. Often violence is perpetrated against members of the group and against other groups.

### **By way of conclusion**

International mass marketing fraud is a global threat to people, companies and financial institutions. By exploring the global financial system, communication networks

---

<sup>6</sup> Victims of fraud are exploited to receive and launder money from other victims or to use false financial instruments, make deposits and transfers or agree to use fake cheques, sell stolen goods, or pay for them with stolen credit cards, or export them and act as a guarantor to foreign companies. (p. 23).



and markets, and by hiding the origin of the operations and illicit procedures, this fraud compromises legal businesses as unaware supporters of criminal activities. Organized crime increasingly initiates, facilitates and profits from this fraud, extracting billions of dollars from vulnerable consumers worldwide. Schemes change and adapt to mislead investigations and to respond to consumers who become aware of fraud schemes.

In short, with regard to the nature, scope and impact of Mass Marketing Fraud, researchers warn of this global criminal threat that involves tens of billion dollars per year. For the victims, the danger extends beyond the loss of funds or savings, and may include risks or physical injury, loss of homes, depression and even the possibility of committing suicide.

This fraud has a substantial impact on the economy and markets by undermining consumer confidence and the legitimacy of businesses. This is an international crime conducted by mafia organizations.

On methods and techniques, one can say that it is becoming increasingly international, involving alliances between groups and billions of dollars annually. Victims are contacted by all types of communication (mail, Internet, telephone, TV, radio) and in person, using different resources that the legal authorities find difficult to detect. The fraud covers legal businesses, mailing lists, several types of communication, multiple payment methods, false identity documents and forged financial instruments, including lotteries, cheques, cash and employment contracts. Fraud agents adapt and change methods and techniques quickly to escape justice and suspicious customers, and to reduce the chances of being found out.

Identity and laundering are the crucial points of the schemes, and a disturbing option is to use victims to receive and launder funds or to receive and apply false financial instruments. Being a non-violent criminal activity, violence can be exercised over non-cooperative victims, within criminal groups or between mafia groups.

According to the report, to fight it will require five globally coordinated international measures and the following:

- 1)** expanded capacity to bring together intelligence services to cooperate in all aspects of the scheme and of its participants;
- 2)** develop the capacity to intercept the operations of mass marketing fraud schemes through legal methods (e.g. filing counterfeit documents);
- 3)** educate the public and assist potential victims to recognize fraud and take action to minimize losses;
- 4)** increase effective measures to identify and promptly assist victims with public and private funds;
- 5)** develop coordinated efforts among investigators, law enforcement agencies and regulatory entities to use power of coercion against perpetrators of the mass marketing fraud scheme.





### **ANNEX: Types of mass marketing fraud (pp.26-29<sup>7</sup>).**

Mass marketing fraud includes an extensive array of false and deceptive schemes to steal money from companies and individuals, properties, information or services. Some schemes are well-known, but due to their proven effectiveness, they are recycled and adapted, in nature and implementation, to the target population. The most profitable and efficient are reproduced, as the crime profits from the delay in recognizing the fraudulent proposal. The versions of schemes most frequently reported to authorities and consumer protection agencies in Africa, North America, Australia, and Europe are as follows:

**Emergency assistance:** The swindler contacts the victim pretending to be a friend or relative of the victim, asking for urgent help, as the victim's family member has been arrested abroad and needs to pay bail, or has had an accident and must repay medical expenses.

**Fraudulent acquisitions or warnings to target companies:** companies are a favourite target of fraud because the amount of money at stake is higher than that involving fraud with individuals, and because it is easier to deceive an employee. One technique used is the "sham sale": it involves convincing the employee that someone in the company has authorized a purchase and, through false documents and phone calls, requiring payment. A variant is to show up as a vendor from a well-known supplier company and request the return of surplus or defective products, aware of the absence of the sales director or of Internet adverts, to the extent of selling them at higher prices.

**Calls for charitable causes:** request for false financial contributions taking advantage of touching humanitarian causes, such as environmental issues, disasters, and holidays for special groups. Even if the money is delivered to the cause in question, some of it will be diverted for personal enrichment or other purposes.

**Forged cheques** (including transfers or powers of attorney): a variety of false lotteries or online auctions involve using false cheques or money to strengthen the look of it being legal transactions. Money or a cheque is sent to the victim as a lottery win or as payment for a high value asset, like a car, so that it can be deposited in the victim's bank account and part of it subsequently transferred to the con person as commission for the "help" given. Sometime later, the bank will inform the victim that the cheque was a fake and that he/she would need to return the entire amount.

A different scheme consists of presenting oneself to an attorney or lawyer as a representative of a foreign company requesting legal assistance to collect arrears. As the representative of the foreign company, the lawyer requests the alleged debtor to pay, receives the corresponding money, and sends the corresponding money to the scammer, after having deducted the legal costs. A variant of the scheme is to show up as the representative of a widow or divorcee and claim the corresponding part of the agreement or inheritance.

---

<sup>7</sup> International Mass-Marketing Fraud Working Group, June 2010, *Mass-Marketing Fraud: A Threat Assessment*, <http://www.ice.gov/doclib/cornerstone/pdf/immfta.pdf>



**Clairvoyants:** Victims are told of an event that will change their lives, in exchange for a prepayment. Seduced by the omen of good fortune or due to threats of setbacks, people agree.

**False services companies:** Just like the false representations of sale of goods, this scheme involves offering false services, such as Internet and communications, medical services, insurance, energy, cars, immigration and residence permits, financial services such as credit protection, replacement support, debt management etc.

**Investments:** It is a variant of the *Ponzi*, and consists of fraudulent promises of high returns in exchange for advanced money for the "opportunity to join" or "help" to buy a "bargain", such as shares or interests in businesses, like oil wells, strong currency or jewels, etc.

**Lotteries or false games:** The impostor presents himself to a person, often with false financial instruments, to convince the victim to pay or advance some money, or to pay the fees and costs, of a supposedly winning lottery ticket or false game.

**"Recovering debts":** Often posing as lawyers or government or legal representatives, the impostor offers victims the possibility of helping to recover a debt in exchange for advanced payment of expenses.

**Romance:** the victim is picked up in a social networking site to fake a romantic interest. Once the relationship and the affection are secure, the victim is asked for cash or marketable goods amidst regular intimate conversations and exchange of gifts. Some victims have reported having sent money to obtain travel documents and buy the airfare ticket, pay for a hospital stay to recuperate from illness, help a charity programme or assist the impostor to recover from a financial difficulty. Since all these schemes represent heavy psychological burdens for the victims, they end up emotionally shattered.

**Sales of goods by false representatives:** A range of false schemes leads potential buyers to purchase products or services over the Internet: auctions, catalogues, purchase orders, classified ads, etc. It is a purchase promise, often at reduced prices or to companies "in trouble", of goods that never arrive, or arrive but are defective, or are different from what had been promised, or have a lower value than that charged. The product or service can be virtually anything: technologies such as iPhones, digital cameras or video game consoles are the most popular. Other products include pets, specialist journals, job vacancies, holidays, health products, precious stones, and metal surpluses. Often victims are invoiced and requested to pay compensation or charged with legal action to collect the fraudulent debt. There is still the case when the legal website of the product is used to offer the victim a second chance, but payment is then made using a dubious form of payment or bank transfer.

**Sale of overpriced goods:** In this scam, the scammer sends fraudulent payments using false documents or money to buy expensive products or services, such as cars, computers or electronic goods. Generally, payment is higher than the cost of the product, and the scammer asks the seller to deposit it and transfer the difference to him electronically. Sometimes stolen credit cards are used. The authorities have noticed that often these companies hire criminals to recover the large amounts at stake.





### **How to cite this Note**

Tapia, René (2012). "Organized crime makes swindling go global". Notes, *JANUS.NET e-journal of International Relations*, Vol. 3, N.º 1, Spring 2012. Consulted [online] on date of last visit, [observare.ual.pt/janus.net/en\\_vol3\\_n1\\_not4](http://observare.ual.pt/janus.net/en_vol3_n1_not4)