AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 200

Red Flags of Fraud

Peter Grabosky and Grace Duffield

Building on an earlier Trends and Issues paper, "The Psychology of Fraud" (No. 199), this paper identifies warning signals for fraud, and proposes some preventive or pre-emptive action. Four fraud types are examined:

- *entrepreneurial fraud;*
- *client or employee fraud;*
- *direct interpersonal fraud (face-to-face); and*
- *indirect mass fraud.*

Examples of each of these are evident in our daily lives and there are often warning signals. Not all of these "warning signals" are necessarily precursors to fraud, but it should be noted that the most productive investment in fraud control is likely to involve strategies which reduce opportunity and enhance guardianship. The setting or context in which fraud may occur can be more or less conducive to offending. This paper aims to enhance our understanding of the situational elements of fraud risk, to permit the design of effective fraud control systems.

Adam Graycar
Director

Introduction

Fraud, like all crime, is the product of three factors: a supply of motivated offenders; the presence of a prospective victim or target; and the absence of a capable guardian (Cohen & Felson 1979). This general rule applies whether one is referring to fraud against government benefit programs, fraud against elderly people, or misappropriation of corporate assets by a company director.

A previous essay (Duffield & Grabosky 2001) explored the motivational basis of fraud. It concluded that a number of psychological factors may be present in those persons who commit fraud, but that they are also associated with entirely legitimate forms of human endeavour. Moreover, technologies of prediction remain imperfect.

This paper will look at what are commonly called "red flags" or indicators of fraud (Krambia-Kapardis 2001, pp. 49–52). These indicators are not inevitably or universally associated with fraud. Rather, their presence suggests a degree of fraud risk. Conversely, their absence is no guarantee that a situation or circumstance is "fraud-proof". But when these indicators are present, the risk of fraud is high, and a degree of caution or extra preventive measures may be appropriate.

For analytical convenience, we will follow the same basic outline as we did in our earlier paper "The Psychology of Fraud" (Duffield & Grabosky 2001). First, we restate our typology of fraud, then we discuss our general indicators of fraud risk. We then discuss those red flags which are more specific to particular fraud types.

We categorise fraud in terms of the organisational context in which it occurs, and the nature of the relationship between offender and victim:

- Fraud committed against an organisation by a principal or senior official of that organisation. Examples of this include offences against shareholders or creditors by errant "high-flying entrepreneurs" (Sykes 1994) or corrupt practices by senior public officials.

March 2001

ISSN 0817–8542
ISBN 0 642 24225 9

Queensland Government
Department of the Premier and Cabinet

Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

- Fraud committed against an organisation by a client or employee. This category includes embezzlement, insurance fraud, tax evasion and other fraud against government.
- Fraud committed against one individual by another in the context of direct face-to-face interaction. This would include classic "con games" (Maurer 1940), customer frauds by sales staff, and predatory activities against clients or customers by fraudulent investment advisers, roof repairers and others who prey directly on a consumer.
- Fraud committed against a number of individuals through print or electronic media, or by other indirect means. This would include Nigerian advance fee frauds (Smith, Holmes & Kaufmann 1999), share market manipulation, and deceptive advertising or investment solicitations pitched at a relatively large number of prospective victims.

General Indicators of Fraud Risk

In the broadest terms, the fundamental red flag of fraud is the anomaly—a variation from predictable patterns of behaviour or, simply, something that seems out of place.

Anomalies can be behavioural, statistical or organisational. By behavioural anomalies, we refer to unusual patterns of behaviour such as living beyond one's means or, more generally, to sudden changes in one's activity. The classic example is the person who begins to lead an extravagant lifestyle, incommensurate with his or her legitimate income. While this does not indicate with absolute certainty that the lifestyle in question is supported by the proceeds of fraud (indeed, the individual in question could be a drug dealer, or the innocent recipient of largesse by a wealthy benefactor such as a deceased parent), it does suggest the possibility.

In our accompanying essay on the psychology of fraud, we identified certain activities which may well contribute to financial stress, thereby providing a motive to commit fraud. Excessive gambling and substance abuse (particularly of relatively expensive illicit substances such as heroin and cocaine) are activities which may be associated with fraud.

Anomalies can also be statistical; when tax deductions for work-related travel expenses exceed a certain proportion of one's gross income, the figures will begin to "stand out". Again, such claims may be entirely legitimate. But they may indicate something to the contrary. Other statistical incongruities which may be indicative of fraud include dramatic unexplained variations in share prices, unusual billing patterns on one's credit card, and atypical calling patterns on one's telephone account. Another would be when a merchant's ratio of loss to turnover is exceptionally high.

By organisational anomalies, we refer to characteristics of an organisation which differ markedly from those generally regarded as best practice. These departures from conventional standards can entail such characteristics as poor leadership, inadequate systems of communication within the organisation, and the lack of transparency to outside observers. The absence of financial control systems, or a board of directors hand picked by the chief executive officer (CEO) and lacking in independent members, may indicate opportunities for fraud which would otherwise not exist. Similarly, unrealistic organisational goals or sales targets, and incentive structures based on commissions, may invite individuals to cut corners (Levi 1995).

Various means of anomaly detection, from simple human observation to the development of complex technologies such as those based on artificial intelligence and neural networking to identify atypical transaction patterns, have become standard means of fraud control. But the absence of anomalies does not necessarily indicate the absence of fraud. Indeed, the most astute fraudsters go to great lengths to not stand out (Sparrow 1996). For this reason, complementary methods of fraud detection, such as random audits and "hotlines" for reporting by knowledgeable third parties, may also be encouraged.

Indicators of Risk for Basic Fraud Types

Entrepreneurial Fraud

When things are going well for the entrepreneurial fraudster, it may be difficult to detect his or her transgressions; but when things go sour, the cracks which begin to appear in a façade of invincibility may indicate underlying pathologies.

Although entrepreneurs and their businesses may suffer from sheer bad luck, specific events may signal something more sinister.

A downward trend in a company's earnings, reduced cash flow and excessive debt may indicate innocent misfortune, managerial incompetence or criminal exploitation by an entrepreneur of his or her organisation's assets. A sudden, unexpected reversal of a company's fortune may be particularly suspicious. So too may a sudden change in auditors. Firms in the midst of financial distress switch auditors more frequently than healthy companies (Apostolou & Crumbley 2000). There may be great temptation to replace an auditor who could be on the verge of discovering something embarrassing or incriminating.

The absence of critical, questioning, external directors on a board may also merit concern. Situations in which the chief executive himself appoints outside directors suggests the possibility that these recruits may be "yes men" willing to turn a blind eye to inappropriate conduct on the part of the CEO. This may especially be the case where the roles of chairman and

CEO are combined and where that person is the principal founder of the business. Such persons often find it difficult to shift from owner to accountable executive, and treat the business as their own.

Additional circumstances which might provide grounds for suspicion are the existence of actual or apparent conflicts of interest on the part of the CEO or other directors. Situations in which directors have private business dealings with, or receive loans from, the company (so-called "related party transactions") may also warrant closer scrutiny. So too is the degree of openness of the share register. If most of the shares are "closely held" by a few major shareholders, they may be inclined to act as if the company's assets were their own.

(For an overview of entrepreneurial fraud during the "decade of greed" in Australia, see Sykes 1994.)

Client or Employee Fraud

The situational indicators of client or employee fraud will vary with the nature of the relationship of the individual to the organisation. Let us look first at fraud by an employee. In order to conceal his activities from the scrutiny of others, the embezzling employee may work long hours and never take a vacation. An employee on the lookout for fraud opportunities may be unusually inquisitive about those aspects of a company's operations involving payments or purchases. After executing a fraud, an employee may resign abruptly or unexpectedly (prior to his theft being detected).

At the organisational level, accounting practices may be lax or unconventional, and financial control systems may be weak or non-existent in a company or government department that is vulnerable to fraud. Most responsible organisations, for example, require that company cheques be signed by at least two individuals.

In contrast to fraud by an organisational insider, client fraud may leave a more immediately visible trail. The perpetrator of insurance fraud may have insured his property for an amount significantly in excess of its replacement value, or may have filed a claim very soon after taking out a policy. The claims of individuals or businesses who are experiencing significant economic adversity may also attract particular scrutiny. Records or documentation of claimed losses may be incomplete.

Telecommunications-related fraud may also be reflected in "red-flag" activities. These can include:

- long-distance access followed by reverse call charges accepted from overseas;
- high-volume usage over short periods before disconnection;
- a large volume of calls where one call begins shortly after the termination of another; and
- the non-payment of bills.

The more sophisticated systems of fraud detection flag long-duration calls, check high international direct dialling call usage and adopt customer "fraud scoring". National telephone carriers such as Telstra can compare "normal" telephone usage to a particular customer's usage, factoring that data into the customer's date of birth, occupation, location, credit details and other indicators to arrive at a percentage risk of fraud by that customer (Grabosky, Smith & Dempsey 2001)

Credit card fraud may also be associated with certain behavioural characteristics on the part of the prospective "purchaser". These may include lack of cost consideration and unusual impatience, multiple purchases of the same product, avoidance of items requiring delivery, and selection of items which could be readily re-sold for cash, such as VCRs and video cameras (Masuda 1993).

Similarly, a sudden escalation in requests for credit references and the velocity of plastic payments, or a high volume of transactions on a credit card within a very short time frame but over a wide geographic area, may indicate the use of stolen credit card details.

In general, the absence of general safeguards and control systems in an organisation are indicative of fraud risk, whether at the hands of "insiders" or "outsiders". Standards Australia has developed a generic standard for compliance systems (AS 3806-98) which provides a valuable framework based on demonstrated commitment from top management, regular performance assessment and clear channels for reporting problems. Smith (1998) identifies current best practice in fraud prevention, including pre-employment screening, transaction monitoring and technologies of authentication.

Direct Interpersonal Fraud

Fraudulent door-to-door sales or solicitations, or similar contacts made over the telephone, may contain elements which differentiate them from legitimate approaches. Whether they entail bogus "roof repair" frauds, or fraudulent charitable contributions, fraudulent pitches are sometimes recognisable.

While a friendly, personal demeanour is entirely appropriate for any interpersonal encounter, one should be wary when greeted with what appears to be undue familiarity, particularly by a stranger. Similarly, one should be wary when approached by a complete stranger and offered what appears to be a windfall. Why, one might well ask, would a person offer a stranger a "hot tip" on a horse race?

Even more indicative are sales pitches which are accompanied by frantic claims of limited availability, pressure to pay in advance or with undue haste, or pressure for an immediate response on the part of the purchaser. Preference for payment in cash, as opposed to cheque or credit card (where the victim may be able to stop payment), may also be regarded as a warning sign. So too may be the existence of confidentiality clauses, which would prevent the victim from disclosing the "special offer" to others.

The decreasing cost of telecommunications has greatly facilitated telemarketing fraud. Personal investment solicitations can now be made over the telephone by complete strangers on the other side of the world. Such calls, especially when accompanied by high pressure sales tactics, are inherently suspect. Sufficient information on which to base a reasoned investment decision is usually unavailable. Moreover, overseas fraudsters may lie beyond the reach of Australian law enforcement and regulatory agencies.

Fraudulent "home repair" services may also have a number of distinguishing characteristics. One should be especially cautious if the contractor comes door-to-door or seeks one out, and offers his or her services at an extremely low price, because he or she "just happens" to have material left over from a recent job. One should also be wary if a contractor is unable to provide a telephone number at which he or she may be contacted and is instead only contactable by leaving messages with an answering service. A request for payment "up front" and in cash may be indicative of the "contractor's" intention to disappear.

Another form of fraud is that carried out by persons who purport to represent charitable organisations. Those who make charitable solicitations on a face-to-face basis but who lack convincing, appropriate identification with the charitable organisation in question may be suspect. Those who solicit by telephone should be prepared to send further details by post. In either event, reluctance to provide the prospective donor with a telephone number of the organisation in order to check the bona fides of the solicitation should also arouse suspicion.

Individuals should be most wary of propositions inviting their participation in activities which themselves are of questionable legality. Invitations to join schemes or deals that appear to contravene the law may be both genuine and illegal. But others may not even be genuine. Many classic con games were based on ostensibly fixed gambling events. Illegal tax evasion schemes have also served as the basis for defrauding those who themselves would defraud the Tax Office. Fraudsters will appreciate that a person defrauded in the context of a patently illegal venture is less likely to report to the police.

> Consumers receive an unsolicited postcard advising that a "multi-item shipment" is being held in a warehouse "ready for you to claim". The card indicates the shipment comprises household, personal and miscellaneous goods valued at over $200 and the consumer could receive a dishwasher, food processor, stereo CD component centre, BBQ or a microwave oven. Consumers are asked to send a cheque for $39.95 or credit card number and the goods will be sent. Offer is valid for 11 days only.
>
> (Source: South Australian Office of Consumer and Business Affairs)

In any encounter, whether face-to-face or over the telephone, one should also take note of what appear to be evasive or defensive responses to questions.

In some cases, third parties may be in a position to identify indicators of interpersonal fraud. Smith (1999) observes that some Canadian banks keep a watch on the accounts of elderly customers and may seek confirmation of unusual transactions which might arise as the result of the senior person being the victim of a con.

Indirect "Mass Fraud"

It has now become trite to suggest that "if an offer appears too good to be true, it probably is". Such offers are also characteristic of indirect, impersonal frauds. At times, these may entail hyperbole verging on the fantastic. Where the offer is communicated through print or electronic media, the message may also be accompanied by dazzling presentation, excessive use of capital letters, dollar signs and exclamation points (e-ezstreet.com 2000). Whatever the medium through which they are communicated, unbelievable bargains, or promises of immense returns for no risk, should always be regarded with healthy suspicion.

The South Australian Office of Consumer and Business Affairs provides summaries of many such solicitations (http://www.ocba.sa.gov.au/scamex.htm).

The credibility of "get rich quick" appeals may appear more realistic in a climate of irrational exuberance. During the recent "dot.com" binge on world share markets, where speculative trading in the shares of small IT companies resulted in astronomical profits for some investors, hyperbole or deliberate misinformation was more convincing than has been the case since the bubble burst in April 2000. "High-tech hype" is now viewed more skeptically.

A common form of fraud is the pyramid scheme. While there are many variations on the pyramid scheme, they tend to follow a pattern which is usually recognisable. The essence of a pyramid scheme is that one's financial reward is conditional upon recruiting others into the scheme. This, combined with a "joining fee", should alert the prospective victim to the nature of the enterprise.

Pyramid schemes collapse when they fail to recruit enough additional participants, with the most recent recruits suffering the greatest loss.

Even without a joining fee, further skepticism may be warranted when one is offered discounts for finding other customers, or where one is pressured for an immediate decision.

Small businesses may also be targeted for mass frauds. Particularly common is false invoicing, where the fraudster sends an invoice for an unauthorised advertisement in a

business directory which is either non-existent or has a very limited distribution. A small business whose principals keep poor records may be more vulnerable to this type of fraud.

The Internet abounds with sites that warn against consumer fraud. Most notable in Australia is the Australian Competition and Consumer Commission (http://www.accc.gov.au/consumer/fs-consumer.htm).

The Australian Securities and Investments Commission's "Gull Awards" identify some of the more prominent questionable investment opportunities (see http://www.asic.gov.au/).

For a list of publications which may assist in identifying possible fraudulent sales, see http://www.emich.edu/public/coe/nice/fraud.html.

Conclusion

As we noted in our previous essay (Duffield & Grabosky 2001) there is no perfect means of predicting who will commit a fraud. Similarly, we conclude here that there is no perfect means of predicting when or where a fraud will be committed. All that we can predict with certainty is that there will always be a supply of motivated offenders and, as long as there is commerce, there will always be opportunities for fraud. To the extent that one's vigilance is relaxed, fraud will be easier to commit. Briefly outlined below are strategies for the prevention and control of the four basic dimensions of fraud which we have identified.

Entrepreneurial Fraud

The most effective means of combating entrepreneurial fraud is to improve corporate governance. Ideally, a regulatory framework will require maximum feasible transparency in a company's or organisation's operations. Such a framework will include disclosure requirements and provisions for shareholder scrutiny. A board of directors which is (and is seen to be) independent of the CEO should also be encouraged.

The role of auditors and legal advisers in the prevention, detection and disclosure of entrepreneurial fraud is also important. These professional advisers must be discouraged from turning a blind eye to client illegality. Banks and other lending institutions, and institutional investors generally, are well situated to exercise a degree of vigilance over a company's internal operations. A strong and independent news media, free of constraints currently imposed by the law of libel, is also in a position to provide a degree of guardianship.

Employee or Client Fraud

Fraud by employees may be most effectively prevented by careful recruitment of staff, responsible personnel management to maintain workplace morale, and by the design of systems to reduce opportunities to commit fraud. Good human resource management is paramount. Ideally, the individual employee will see his or her contribution as an important part of the organisation's success, and will see the organisation's achievements as indicative of personal success. Fraud by clients may also be discouraged, if not prevented, by making the client's entitlements and responsibilities clear and explicit, and by treating the client fairly and respectfully. In the event that fraud is perpetrated by employees or by clients, systems should be in place to detect inappropriate transactions. Because the most effective fraudsters take great pains to cover their tracks, a degree of random inspection or auditing will also be important.

Face-to-Face Fraud

Although confidence men may portray their victims as corrupt and greedy (as discussed in Duffield & Grabosky 2001) many of these victims are somewhat passive people who were either naïve or indiscreet in money handling. In some cases they were also found to be lonely and depressed. This was particularly characteristic of elderly women who were victims of face-to-face

In November 2000, Crime Prevention Queensland in the Department of the Premier and Cabinet initiated three fraud prevention projects targeted at specific Queensland communities. These projects, supported by a grant from *National Crime Prevention—Towards a Safer Australia* (an initiative of the Federal Government) and coordinated by the Queensland Office of Fair Trading, are:

- Protecting Seniors Against Mail Fraud, focusing on Toowoomba and the Sunshine Coast;
- Campaign Against "Blowers"—Invoice Fraud, focusing on the Logan area; and
- Heads Up, consumer fraud prevention targeting the Gold Coast.

Using crime prevention principles, the projects target a specific community problem and seek to involve these local communities in developing local responses in a systematic and planned way. The projects involve each community in identifying its problems and priorities, designing response strategies and planning their implementation. A key feature will be the design and dissemination of education materials to raise community awareness of these types of consumer fraud.

Expected outcomes include the enhanced capacity of the community to protect itself from fraud, a better informed and equipped community to respond to fraud attempts, an improved capacity of law enforcement agencies to detect and prosecute consumer fraud, and higher reporting of attempted and actual frauds.

See also the Queensland Office of Fair Trading web site: http://www.fairtrading.qld.gov.au/.

(Source: Queensland Government)

fraud (Blum 1972, p. 69). Regardless of the fact that some people in the community seem to be more vulnerable to face-to-face fraud than others, the most effective bulwark against face-to-face fraud is to educate prospective victims about the risks which they face. Consumer awareness is the first line of defence, and responsibility for this must be widely shared. First and foremost, the individual consumer has a responsibility to become informed of the risks involved in commercial transactions, and of what steps to take to protect oneself. Government agencies and industry associations are ideally situated to impart information to consumers and to alert them to pitfalls in the marketplace.

Indirect, Impersonal Fraud

As is the case with face-to-face fraud, consumer awareness is paramount in combating indirect fraud and, again, this task must be shared. A degree of government effort, such as that typified by the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission, remains essential. These agencies warn investors and consumers of risks in the marketplace, and can take enforcement action in the event of an offence. Legitimate businesses and their associations, such as the Australian Direct Marketing Association (http://www.adma.com.au/consumer/default.htm) also provide advice to consumers. By publishing a list of member companies that abide by the ADMA code of practice, the association is able to direct consumers towards reputable businesses.

Since most impersonal fraud is directed at a large number of people, the possibility of detection may be greater. Regular "patrolling" of the media and cyberspace, combined with the establishment of effective channels for the reporting of "offers too good to be true", have become standard practice in many jurisdictions. For example, the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission regularly sweep the Internet to check for compliance with consumer protection principles in electronic commerce. They fill the dual role of educating business about best on-line practice and educating consumers about how to evaluate an offer.

In summary, the challenge lies in structuring systems to limit the access of the potential fraudster to a target, without unduly impeding legitimate commercial activity. If fraud does occur, methods must be in place to ensure that it is speedily detected. Appropriate sanctions should be in place to deter the offender, and others who would follow in his or her footsteps.

Acknowledgments

The Fraud Offender Characteristics project was funded by National Crime Prevention—Towards a Safer Australia, an initiative of the Federal Government. It was initially proposed by Crime Prevention Queensland in the Department of the Premier and Cabinet.

The authors wish to thank Keith Inman, Michael Levi, Tim Prenzler and Russell Smith for their helpful comments.

References

Apostolou, N. & Crumbley, D. 2000, *Forensic Investing: Red Flags*, http://www.bus.lsu.edu/accounting/faculty/napostolou/forensic.html#Red Flags (visited 28 December 2000).

Blum, R.H. 1972, *Deceivers and Deceived: Observations on Confidence Men and their Victims, Informants and their Quarry, Political and Industrial Spies and Ordinary Citizens*, Charles C. Thomas, Springfield, Illinois.

Cohen, L. & Felson, M. 1979, "Social change and crime rate trends: A routine activity approach", *American Sociological Review*, vol. 44, pp. 588–608.

Duffield, G. & Grabosky, P. 2001, "The psychology of fraud", *Trends and Issues in Crime and Criminal Justice*, no. 199, Australian Institute of Criminology, Canberra.

e-ezstreet.com 2000, *Common Fraud Red Flags*, http://www.e-ezstreet.com/Shopping/ShoppingHelpful_Hints/shopFraud_Red_Flags/shopfraud_red_flags.html (visited 28 December 2000).

Grabosky, P., Smith, R.G. & Dempsey, G. 2001, *Electronic Theft: Crimes of Acquisition in the Digital Age*, Cambridge University Press, Cambridge.

Krambia-Kapardis, M. 2001, *Enhancing the Auditor's Fraud Detection Ability: An Interdisciplinary Approach*, Peter Lang, Frankfurt am Main.

Levi, M. 1995, "White collar crimes and other crimes of deception: Connecting policy to theory", in Barlow, H. (ed.), *Crime and Public Policy: Putting Theory to Work*, Westview Press, Boulder, Colorado, pp. 247–68.

Masuda, B. 1993, "Credit card fraud prevention: A successful retail strategy", in Clarke, R.V. (ed.), *Crime Prevention Studies*, vol. 1, Criminal Justice Press, Monsey, New York, pp. 121–34.

Maurer, D. 1940, *The Big Con: The Story of the Confidence Man*, Anchor Books, New York.

Smith, R.G. 1998, "Best practice in fraud prevention", *Trends and Issues in Crime and Criminal Justice*, no. 100, Australian Institute of Criminology, Canberra.

Smith, R.G. 1999, "Fraud and financial abuse of older persons", *Trends and Issues in Crime and Criminal Justice*, no. 132, Australian Institute of Criminology, Canberra.

Smith, R.G., Holmes, M.N. & Kaufmann, P. 1999, "Nigerian advance fee fraud", *Trends and Issues in Crime and Criminal Justice*, no. 121, Australian Institute of Criminology, Canberra.

Sparrow, M. 1996, *License to Steal: Why Fraud Plagues America's Health Care System*, Westview Press, Boulder, Colorado.

Sykes, T. 1994, *The Bold Riders: Behind Australia's Corporate Collapses*, Allen and Unwin, Sydney.

Dr Peter Grabosky is Deputy Director of the Australian Institute of Criminology.

Grace Duffield is a psychologist with the Australian Security Intelligence Organization.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.