Organized fraud and organizing frauds : Unpacking research on networks and organization

Michael Levi

Criminology and Criminal Justice 2008 8: 389
DOI: 10.1177/1748895808096470

Criminology & Criminal Justice

www.sagepublications.com
ISSN 1748–8958; Vol: 8(4): 389–419
DOI: 10.1177/1748895808096470

Organized fraud and organizing frauds:
Unpacking research on networks and organization

MICHAEL LEVI[1]
University of Cardiff, UK

Abstract

This article examines the settings for frauds in the context of crime networks, fraud opportunities and of a victim-centric typology of fraud. It demonstrates the variety of actors, settings and the variable need for knowing collaboration between co-offenders in frauds of different types. It explores what is known about those involved in the organization of some forms of frauds; how they find both co-offenders and victims in face-to-face and remote settings; and the barriers to growth of the 'fraud business'. It concludes that the globalization of crime is part of contingent relationships between settings, with their rich and varied opportunities (reflecting patterns of business, consumer and investment activities), the variable abilities of would-be perpetrators to recognize and act on those opportunities (the 'crime scripts' perspective), and their interactions with controls (including, but not restricted to, law enforcement). Constructs of 'organized crime' are becoming less obsessed with the structure of groups than with what people need from the largely illicit and largely licit worlds before they commit fraud. Although some frauds are committed by generic transnational 'organized crime' networks, others are merely mobile small groups or individuals who can transplant techniques wherever they go; and others still commit very large one-off frauds without a need for long-term or any involvement in 'organized crime'.

Key Words

crime and ethnicity • cross-border crime • identity fraud • organized crime • policing • white-collar crime

Introduction

The analytical and research literature on fraud is much sparser than that on organized crime generally or drugs trafficking in particular.[2] This partly reflects its relatively low political valuation as a non-core part of 'the crime problem', which in turn affects research funding. But the relative (in)accessibility of fraud networks to outsiders is also a factor, since frauds (and other crimes) differ in the way that they are open for marketing, and in the interaction between the parties. In this article, we examine the settings for frauds, which both frames and reflects networks, in the context of fraud opportunities and of a victim-centric typology (Table 1, adapted from Levi and Burrows, 2008). This demonstrates the variety of actors, settings and (less clearly) need for collaboration in frauds of different types. In the process, we explore what is known about those involved in the organization of frauds, though the space available (as well as our knowledge) constrains the number of fraud types that can be discussed.

Organizing frauds

Two important themes in analysing the extent to which crimes are loosely or tightly organized are (1) the ease with which willing criminals find the co-offenders necessary or helpful for any given set of offences; and (2) the breaking down of the elements of criminal organization into its component parts (i.e. what is termed 'script analysis'[3] by Cornish, 1994; Cornish and Clarke, 2002). These themes also reflect the tension (in this article and more generally—see Levi, 2007) between writing about the personnel involved in frauds (the networks) and what it takes to commit frauds (the scripts). It is helpful to think of the tasks that need to be performed to commit serious frauds (and other crimes) and the range of places where they need to be and are performed. (For all the talk about 'the' globalization of 'crime', some of these tasks are as easily accomplished at a local or regional level as they are transnationally, at least in some jurisdictions.) A higher level 'script analysis' of crime for gain might look like the following, with more specific frauds having their own 'scripts' and variable necessities to find co-offenders.

When analysing the dynamics of particular crimes and/or criminal careers, these procedural elements can be broken down further into much more concrete steps and the relationships between their criminal participants analysed (see e.g. Morselli, 2005; Morselli and Roy, 2008 for some advanced empirical efforts). These steps are not necessarily sequential: for example, we may see a financial crime[4] opportunity only when we meet accountants or lawyers who are able to facilitate it, or we may already have in place all the steps as part of our ongoing 'criminal enterprise'. Criminal finance, some or all criminal personnel or the 'tools of crime' (from non-transparent companies to credit cards) may come from or go to another country, constituting 'transnational' crimes; or else remain within one country, constituting 'national'

Table 1. A typology of fraud by victim category and form of activity

Victim sector	*Victim sub-sector*	*Examples of fraud*
Private	Financial Services	Cheque fraud
		Counterfeit intellectual property and products sold as genuine
		Counterfeit money
		Data-compromise fraud
		Embezzlement
		Insider dealing/market abuse
		Insurance fraud
		Lending fraud
		Payment card fraud
		Procurement fraud
	Non-financial services	Cheque fraud
		Counterfeit intellectual property and products sold as genuine
		Counterfeit money
		Data-compromise fraud
		Embezzlement
		Gaming fraud
		Lending fraud
		Payment card fraud
		Procurement fraud
	Individuals	Charity fraud
		Consumer fraud
		Counterfeit intellectual property and products sold as genuine
		Counterfeit money
		Investment fraud
		Pension-type fraud
Public	National bodies	Benefit fraud
		Embezzlement
		Procurement fraud
		Tax fraud
	Local bodies	Embezzlement
		Frauds on Council taxes
		Procurement fraud
	International (but affecting public)	Procurement fraud (by national against other—mainly but not always foreign—companies to obtain foreign contracts)
		EU funds fraud

Note: See Levi and Burrows (2008, Box 1) for a glossary of common fraud types. The counterfeiting of intellectual property counts as fraud only if the vendor represents it as being the genuine manufacturer's product (or, arguably, if the purchaser believes it to be genuine). Otherwise it may be a loss of the manufacturer's property rights, but no-one is defrauded: the manufacturer loses principally if the purchaser would have bought the legitimate product at the price offered for it, but also if there is collateral damage to the product's reputation.

crimes.[5] In the case of fraud, offenders may start with differential access to local, national or international resources, but the exploitation of inter-state and international regulatory and criminal justice asymmetries—e.g. different levels of enforcement in the states or countries in which the fraudsters operate—represents a positive advantage for fraud compared with most other crimes. In this article, I shall seek to combine the scripts with a brief analysis of the sorts of networks involved in them.

Applying the sort of script found in Box 1, would-be fraudsters have to find 'marks' to target with their schemes,[6] and develop techniques for getting them to part with their money voluntarily: the hallmark of fraud. Some such offences occur (at least in part) face to face; others are done remotely; while others still may start technologically (with a letter or an e-mail) and end with some interpersonal contact. Let us take as an example of the latter '419 frauds', so called after section 419 of the Nigerian criminal code. There are few e-mail users who have never encountered scam e-mails—which usually arrive from a yahoo or hotmail address—offering them vast wealth if only they will help their previously unacquainted banker/relative

Box 1. The process of fraud and other crimes for gain

1. See a situation as a 'financial crime opportunity'
2. Obtain whatever finance is needed for the crime
3. Find people willing and able to offend (if necessary for the crimes contemplated) and who are controllable and reliable
4. Obtain any equipment/data needed to offend
5. Carry out offences in domestic and/or overseas locations with or without physical presence in jurisdiction(s). This will usually involve manipulating—with varied degrees of complexity, technology and interpersonal communication skills—victims' perceptions of 'what is happening'
6. Minimize immediate enforcement/operational risks. Especially if planning to repeat frauds, neutralize law enforcement by technical skill, by corruption, and/or by legal arbitrage, using legal obstacles to enforcement operations and prosecutions which vary between States
7. Convert, where necessary (e.g. where goods rather than money are obtained on credit), products of crime into money or other usable assets
8. Find people and places willing to store proceeds (and perhaps transmit and conceal their origin)
9. Decide which jurisdiction(s) offers the optimal balance between social/physical comfort and the risk of asset forfeiture/criminal justice sanctions. Indifference in any one State or sub-state arena may suffice to neutralize an investigation, and staffing inadequacies as well as corruption may be the cause of official inaction.

of a deceased corrupt dictator put their 'dormant account' or 'unknown to the authorities but at risk' money into their own account for 25–40 per cent of the 'take' (usually $25 billion). Some data can be harvested for 'identity fraud' but the victim is often persuaded to pay 'advance fees' to remove blockages in the funds transfers, and may even be lured to Nigeria or some other country to pay out more. One of the ironies is that Nigerians are utilizing their stereotype of corruption in order to make the proposition more plausible to their intended 'marks'. Such propositions used to be made by letter (sometimes using counterfeit stamps to reduce operating costs) but are now more often made by e-mail, which is almost free. By contrast, other frauds such as lottery scams may have quite elaborate and convincing paperwork delivered by bulk mail, often from Spain: although the authorities may be able to identify such scam letters prior to delivery, legal prohibitions on interference with the mail (plus commercial interests insofar as they are paid by the distributors) prevent them from stopping distribution unless the stamps themselves are counterfeit. Such lottery scams (whether by mail or e-mail) seldom involve interpersonal contact.

We can see from the Box 1 process map (or 'script') one important difference between frauds and most traditional crimes that have victims: at the time when the offence is committed (which, in contrast with other property offences, may happen undetected continuously over years), the fraudster can be but does not normally need to be in the same place or even the same continent as the victims or their property. However, few frauds need to be executed on an international basis, and some fraudsters (like gangsters) have their domestic geographic comfort zones, even to the level of the shops in which they prefer to use stolen cards and those they avoid (Levi, 2003[p1]). It is quicker for a credit card fraudster or telemarketer to get a train from London to Paris than from London to Liverpool, and that can be important when the rate of fraud upon a stolen or counterfeited card is time-critical. Rising fuel costs notwithstanding, it is easy and relatively cheap to fly to many parts of the world, even if one is buying the ticket with a genuine credit card or cash (which may be the proceeds of past crimes). However in many other cases, speed of action is unimportant because there is a long elapsed time between the commission of fraud and its detection by the victim or by a third party: the latter includes American Express, Visa or MasterCard (for payment card frauds); Dun and Bradstreet or Experian (for personal and commercial credit frauds); and the UK Financial Services Authority, Office of Fair Trading and other regulators (for investment frauds, 'market abuse' and consumer scams). Choice of offender or victim location is determined by other factors (such as the large number of relatively wealthy but still anxious elderly people in Florida or the south-east of England). In the larger cases, professional intermediaries and bank accounts are necessary components in presenting a plausible front and in obtaining and laundering the funds; in others, cash may be wired via money service bureaux (like Western Union) or by 'underground banking' (Passas, 2005) to foreign or sometimes domestic locations.

What is different about frauds compared with other crimes? First, as researchers since Cressey (1955) have shown, most professionals are already in a position to commit major frauds such as embezzlement by virtue of their legitimate jobs. (One may add to Cressey's rather individual-oriented approach that few finance directors and CEOs will have their 'instructions to pay' questioned by subordinates: so they too do not need active conspirators—merely that the ciphers they have appointed follow orders.) Second, whether as (i) individuals and/or as (ii) corporate actors, they are less likely to be suspected as being 'out of place'—as Felson (2002, 2006) might put it, their camouflage is already there—both as transactors in the business deal and as movers of illicit funds after the fact. The latter is connected to the third point, which is that most (but not all) frauds obtain money in electronic form, and therefore have less need to deposit and transfer large cash sums, which more readily arouse suspicions among the ever-larger number of bodies (not just banks and building societies but also now antique dealers, car dealers, estate agents, and jewellers), who have a criminal law obligation to report to a Financial Intelligence Unit (SOCA in the UK) 'suspicious transactions'.[7] The imagery of cash and drugs trafficking still predominates in the anti-money laundering arena, despite the expansion of the legal mandate to include all crimes. (See further, Levi and Reuter 2006, 2008.)

One more point is noteworthy. There is a temptation—especially in work on 'organized crime'—to see the stages above as being part of a conscious plan: a preconceived strategy of deception (thus replicating the process of 'case construction' by police and prosecutors when preparing for court). However this can be a mistake. In *The Phantom Capitalists* (Levi, 2008a, originally 1981), I suggested the utility of looking at bankruptcy and other frauds in terms of a threefold typology:

(1) pre-planned frauds, in which the business scheme is set up from the start as a way of defrauding victims (businesses, public sector and/or individuals)
(2) intermediate frauds, in which people started out obeying the law but consciously turned to fraud later; and
(3) slippery-slope frauds, in which deceptions spiralled, often in the context of trying—however absurdly and over-optimistically—to rescue an insolvent business or set of businesses that in reality had no hope of repaying its debts in the future.

In short, motivation to defraud can be heterogeneous rather than a single phenomenon; and (where physical identification is not an issue) planned fraudsters have an interest in pretending to be slippery-slopers or honest-but-unlucky, to minimize the chances of prosecution, conviction and imprisonment, thus reversing prosecutors' case constructions. As with Cressey's embezzlers, existing business people have comparatively little problem in organizing funds transfers out of the company and/or bankruptcy fraud (although the disposal of large amounts of goods very quickly may be difficult—one may need an apparently legitimate or large scale illegitimate

trader to perform a brokerage role in disposal).[8] Once people are willing to risk whatever ethical and social sanctions might be expected,[9] the key practical problem is organizing the escape from criminal sanctions and proceeds of crime recovery by creditors or state. These measures may involve willing collaborators and/or innocent third parties, or a combination (including the coalition of the willing pretending to be innocent and often remaining unchallenged). People can use corporations or professions as a means to attain fraudulent ends, and can do so either at the start (pre-planned fraud) or as an afterthought in a changed situation. The corporations can be substantive and real or mere fronts or shells for the perpetration of fraud. But people can also commit frauds against companies and the government as outsiders or from more junior positions. An example follows:

> Jagmeet Channa, a charity volunteer from a middle-class family and with no previous criminal convictions, who had been employed at HSBC headquarters first on a short term contract 10 months earlier, was sentenced to nine years in prison for attempting to steal £72 million from HSBC in April 2008. One Friday, Channa authorized two seemingly straightforward transactions in transfers to accounts at Barclays in Manchester and Société Générale in Casablanca, using passwords stolen from colleagues. Transcripts of telephone calls made from his HSBC landline that evening reveal a series of calls informing several people that the fraud was a triumph. Attempts to uncover their identities proved fruitless because they were using pay-as-you-go handsets, which were not already being monitored. Just after lunchtime on the Sunday, Channa's plan fell apart. Banking security officials in Malaysia had noted a double transaction, prompting 'cause for concern'. Channa had used a global financial holding account where vast amounts are paid in and then removed. At the close of daily trading, the account should register zero, but Channa had inexplicably forgotten to change it and his holding account was showing a massive debt. It was an elementary error that, if Channa had avoided it, might have allowed him to pull off his record-breaking crime.[10] Channa's decision to execute the crime on a Friday had compounded his mistake. With trading frozen over weekends, security officials find it much easier to detect anomalies. Had Channa committed the fraud during the working week, his scam might have remained undetected for long enough to allow his partners to empty the £72m from the accounts in Manchester and Morocco. The £72m was frozen and returned to HSBC.
>
> (Summarized from *The Observer* and other UK newspapers 13 July 2008 and from the author's interviews with bankers 2008.)

It is not currently known whether Channa was 'planted' at HSBC or was targeted by others after his arrival, but—were it not for the evidence of his phone calls to conspirators—it might have been possible for him to carry out all these things alone or with one or two conspirators rather than as a component of an ongoing 'organized crime group'. As I write, the other crime involvements—if any—of the other parties are unknown. (The sort of analysis conducted by Morselli and Roy, 2008, depends on long-term

surveillance of the networks of people already suspected of serious crime.) This emphasizes the point that fraud permits a variety of offender organizational permutations.

As for the persistence of crime techniques over time, those businesses that during the 1960s and 1970s deceived their creditors, on the basis that they needed larger orders to supply their expanding 'mail order' trade, would now do the same on the basis that they have a booming internet-based sales business, especially prior to Christmas (Levi, 2008a). In the era of the credit card, dishonest merchants might pass large quantities of (i) fake or (ii) genuine (but on stolen card) transactions through their commercial accounts, claim (as is normal with traders) advance reimbursement from merchant acquirer card companies, and then disappear before the card issuer, merchant acquirer or cardholder realizes there has been a fraud at all.[11] Looking more at individual 'purchasers' than businesses, payment cards were rare during the 1970s, but fraudsters can now use credit card numbers skimmed from unsuspecting cardholders to order hundreds of computers on the net from different suppliers, have them delivered to 'drop addresses' in the UK or the US, and then forwarded to addresses elsewhere for resale: all of this before the cardholder or card issuer becomes aware there is anything wrong. (The limited availability of such 'drops' serves as a brake on the exploitation of these and other 'identity fraud' opportunities.) This and other cyberfraud techniques reflect a comparative criminal advantage arising from the combination of high technological skills and high motivation because of poor opportunities in their home countries. There are also large-scale credit card and loan 'bust outs' using people's own and stolen identities to obtain goods and money.

The illustrations above show that behaviour of victims-to-be and 'capable guardians' has to be considered as part of the organization of crime. Some suppliers of goods on credit simply make assumptions about creditworthiness without asking for references (or are satisfied by references from members of the credit applicant's family who had no plausible business dealings with the firm). They may check out the companies on telephone/trade directories such as yell.com or BT and, if they are there, may assume the entries reflect genuine trading, not realizing that they too may have been 'fixed'. If the fraudsters—as companies or as individuals—are buying electronic goods, the sales pressures on telecoms and computer firms are extreme, especially in a global next-day service culture, and the rewards for salespeople are often based on what they sell, irrespective of whether or not it is paid for, though some companies do claw back commission on fraudulent sales, which may act as a brake on enthusiasm or wilful blindness. Creditors in highly competitive industries are reluctant to share their fraud losses with other firms and are afraid publicity may make them more attractive to other fraudsters (author interviews with companies): whether the latter fear is reasonable is unverified. Sharing information anonymously via third parties such as trade reference agencies represents one route to learning from experience. These third parties might

be viewed as 'capable guardians', but what they may see or construct out of their partly automated analytical methods are suspicions of fraud rather than undisputed crimes they have witnessed.

At the *individual* level, prior to the 1960s (as now in faith and other close communities), credit was seen more as a personal trust than as an impersonal risk judgement made by professionals. This is one reason some fraudsters target religious affinity groups, because the approach for investment is then seen as coming from a friend rather than a stranger, where trust norms may not apply (or not to the same extent). Often today, the granting (or refusal) of credit to individuals is driven largely by reports from agencies such as Experian and Equifax (internationally) and—in the UK—Callcredit. These reports incorporate large amounts of prior credit behaviour, as well as county court judgements and bankruptcy/Individual Voluntary Agreement records. To these are added financial institutions' proprietary credit scoring—statistical analysis of aggregate data on past loan experiences ('goods' and 'bads')—and the 'risk appetite' of the lenders, which in the decade before the 'credit crunch' in 2007 was high, due to the relative cheapness of money and the need to find outlets for funds held on deposit if they were to make a profit.

The role of criminal justice in the control of first party credit fraud—where borrowers themselves commit fraud rather than have others steal their details or their cards—is relatively unimportant. Unless the bad debtors change their names and evade indirect identification, credit reference agencies can still incapacitate future credit opportunities, irrespective of whether people have been convicted, discharged from bankruptcy or indeed have avoided going 'bust'. Electronic footprints on individual adults are quite pervasive (especially in the UK and North America, far less so in Asia, Africa and Eastern Europe), and attempts to sidestep these controls on identity thefts and cloning are a key battleground against fraud today. Licit and illicit migration flows generate particular difficulties and asymmetries in the validation of credit histories. For example. the birth registers and other personal identifiers are absent from centralized records in many African and Asian countries, so cannot readily be checked, and certainly not electronically. Many of the features of late modernity upon which 'identity validation' rests are not uniformly available.

Fraud networks: between the opportunity and the criminal act

Tremblay (1993) argued that the likelihood of crime commission is a function of co-offender accessibility and suitability, and Felson (2003) stressed that offender convergence settings 'help likely co-offenders discover one another in the context of their routine activities. Such settings provide an ongoing structure for criminal co-operation, even as participants change. This makes possible a local process of accomplice regeneration, leading to

sustainable criminal behaviour'. Morselli and Roy (2008) note that both script analysis and social embeddedness emphasize purposive social action, but differ inasmuch as the social embeddedness perspective places the social network as the force driving such action, whereas, following Cornish and Clarke (2002: 53), the script approach maintains that 'the shape of criminal organization emerges from the requirements of crime commission', the network being only one of these requirements. The evidence does not enable us to determine whether context or existing networks drive organization. Morselli and Roy argue (p. 77) that the 'main objective of a network analysis of crime scripts … should be to untangle how some participants contribute in varying degrees to keeping the inherent channels of a [crime]script in place' (see p. 83 in their work for a car ringing 'script').

A priori, it would appear that different skill sets and statuses will be needed for different fraud offences, and the barriers to entry depend on the starting point of any given individual or network in relation to the practical opportunity and criminal justice obstacles confronting them.[12] In most countries of the world, a distinction is made between 'laissez faire' opportunities to set up and work in commerce[13] and some restrictions applied to people who want to open or work in the financial services sector, largely on the grounds that the latter can directly steal funds from the public. It is important to understand such restrictions in a global context rather than the traditional nation-state perspective of regulation and criminal justice: Nick Leeson (1997) was refused a licence by the predecessor of the Financial Services Authority because he had failed to declare to it a county court judgement against him on a debt; but Barings gave him a job in the far less controlled atmosphere of Singapore, where—though it is very doubtful he started out with that intent or with a concrete fraudulent plan—he was able to conduct trades that brought down the entire bank. One possibility for 'underworld' offenders is to obtain co-operation from or to put pressure on people in respectable positions in order to use them as tools of fraud (see the Channa example earlier, but also people in much more senior positions). Once they have committed one offence (or legal act that would be seen as highly disreputable), they may find blackmail makes exit difficult. Some frauds can be perpetrated most readily by licensed securities dealers, and persons who are part of or suspected of being connected to a conventional 'organized crime group' would have great difficulty passing the examinations and the 'fit and proper person' test for admission. (This would also require substantial elapsed time to acquire the knowledge, and a longer 'investment' than is normal.) Therefore, one port of entry is to 'do a deal' with existing brokers, as the younger members of New York Mafia families did with some Russian American brokers during the 1990s, against the advice of their elders, who thought it too dangerous to move outside 'the family', whom they could control via ties of mutual obligation (Diih, 2005).[14] Such intergenerational tensions are part of the response to declining market position for traditional 'organized crime', eroded as it was by the undercover infiltration and electronic surveillance, followed by prosecutions

under the Racketeer Influenced Corrupt Organization (RICO) legislation. They chose Russian American brokers because they judged that people of that background were more likely than others to find an approach from 'the Mob' attractive: an example of the irony that a 'bad reputation' can bring in business opportunities.

To illuminate such issues, we must first consider what sorts of networks are needed for different offences, and the extent to which their contacts and skill sets enable them to commit a variety of fraud (and non-fraud offences). For price-fixing cartels, for example, what is needed is an ability to pose as a legitimate bidder (which will usually require them to have experience in a relevant area of business) and trust between 'repeat players' that if they overbid for contracts, the winner this time will overbid later to enable them to win. This is easier within a homogeneous elite—the 'good old boys' (a term that originated in the Southern States of the US)—than among comparative strangers, but such elites can be transnational businesspeople as well as locals. (See Harding, 2007, for a contemporary review.) In more competitive markets, the alternative may be corruption of the contract-giver, perhaps even at the specification stage where the 'spec' can be devised in order to give one party an inbuilt advantage. Cartels use their own corporate and individual identities for contracts (though not necessarily for the secret meetings that precede the bids) and would seldom need any false corporate fronts for money laundering purposes since no illicit money changes hands; but bribe-payers might need some false or genuine trading fronts in order to channel payments to the corrupt public official or private sector beneficiary.

Sometimes what is needed for the accomplishment of fraud is compliant people who do not ask critical questions: this was the case with Nick Leeson and Barings Bank, where as a leading trader, Leeson was surrounded by Singaporean subordinates and colleagues who were passive and with British superiors who understood little about trading and were content to take the results he fed them that fed their own large bonuses (Leeson, 1997). Some corporate fraudsters—such as the late Robert Maxwell and the chiefs of Enron—appoint staff on much higher than normal market salaries to ensure their loyalty or wilful blindness when facing alternative employment on much lower salaries. The circle of conspirators at Enron was larger, but for the main part, they had bankers and lawyers who constructed large numbers of offshore Special Purpose Vehicles, and bright, well paid staff whose jobs would have been imperilled by asking critical questions. Rogue trader Jerome Kerviel of French bank Société Générale may have had an occasional accomplice (as is alleged in 2008), but managed to rack up trading losses of billions in 2007 without the aid of an 'organized crime group', taking advantage of weaknesses in supervision which required the resignation of senior management. All of the above should be borne in mind when thinking about fraud and organized networks: there may be no need for conscious co-conspirators, depending on the chain of authority within large corporate or governmental settings and

their competence. What some offenders are able to do is simply deploy the range of global corporate mechanisms available in a free enterprise society where there are (perhaps tautologically) insufficient 'capable guardians' to stop them misusing the disguises offered by the corporate form or the authority and power of a corporate role. Let us take as an example the career of Robert Vesco (Hertzog, 2003), who died in May 2008, to less than flattering obituaries around the globe.

Robert Vesco

A high school dropout from Detroit, Vesco lied about his age to get a job on a car assembly line. In 1965, Vesco hustled control of a small, failing New Jersey valve-making company in return for a five-year $50,000 IOU. A year later he swapped its assets for control of a defunct stock market-listed company he renamed International Controls Corporation, which rose in the 1960s Wall Street boom. Exploiting heavy borrowing and creative accounting, Vesco used ICC shares to buy bigger companies. But he had to keep doing deals to pay interest and boost the share price. By the age of 30, Mr. Vesco was a millionaire.

He later became involved in a Swiss-based mutual fund company, Investment Overseas Services (I.O.S.), run by a swindler called Bernie Cornfeld (Raw et al., 1971). When I.O.S. ran into trouble, Mr. Vesco offered to rescue the company and was embraced by investors terrified of losing their savings. He bought I.O.S. in 1970 for less than $5 million, gaining control of an estimated $400 million in funds. The accounting at the company had been so chaotic that Vesco was able to plunder its holdings at will. After numerous complaints, the US Securities and Exchange Commission charged him and others in a civil suit with stealing more than $224 million. But he had already fled, first to the Bahamas and then to Costa Rica. There, he established a close friendship with President José Figueres, ploughing some $11 million into his adopted country, especially into a company founded by Figueres, who passed a law to guarantee Vesco would not be extradited. He also befriended a nephew of President Nixon, and gave $200,000 to the Nixon campaign (which allegedly helped fund the Watergate burglary) in the hope that the president would help quash the investigation against him. Eventually, a scandal following one of his high-tech brainstorms—a factory to make machine guns, which included President Figueres's son as a partner—led to his flight to the Bahamas, where he invested in the then Prime Minister. He was welcomed in Antigua and Nicaragua, before Cuba finally accepted him for 'humanitarian' reasons: of course there was no extradition from there to the US. Vesco eventually upset the Castro government with a scheme to produce a wonder drug that supposedly cured cancer, AIDS, arthritis and even the common cold. He was jailed for 13 years for defrauding a state-run biotechnology laboratory run by Fidel Castro's nephew, Antonio Fraga Castro. If we examine this remarkable life—and the lives of other transcontinental fraudsters (Block, 1991; Block and Weaver, 2004)—we can see that the

tools of Vesco's trade—and his network—were his charisma, accountants and lawyers willing to create legal entities to serve his interests (especially in a period before money-laundering legislation imposed greater due diligence requirements on them), a level of wealth that enabled others to 'party' at his expense, and his ability to hone in on corruptible people who could offer him protection from other governments and creditors pursuing him through the civil courts.

Enron

In the last year at Enron Global Finance group, managers were sometimes handed a list of Enron assets and instructed to go out and sell some to the Special Purpose Vehicles. A manager would pick something, from a plant to stock to a piece of a start-up company, then discuss the deal with a team of internal lawyers and auditors. A bank or other investor lent money to the newly created company to finance the purchase. The new company, in turn, paid the money to Enron. The use of an intermediary was to make the loan belong to the new company, not Enron, and thus not to count as a debt on Enron's financial statement.

Instead, it counted as income to Enron when the new company passed on the proceeds.

Less debt and more income assured Enron would keep its high credit rating (making borrowing cheaper) and would keep the stock price up.

Top graduate school employees told the *Houston Chronicle* (20 January 2002)[p3] there were many uses for the vehicles they considered legitimate, such as bringing in outside partners to share the risks of a particular venture: but there was little question, especially toward the end, that many had no real 'business purpose' other than improving financial appearances. Say the asset was 100 shares of IBM stock. Enron would divide each share into two parts, one called a 'control interest' and one called an 'economic interest'. Then it would sell the economic interest to a newly created Special Purpose Vehicle. The asset was rarely as simple as 100 shares of another company's stock. So Enron had to put a value on it. Because there was no real outside buyer, it decided the price itself and had that number approved by its auditor, Arthur Andersen.

The deal was placed with a bank, insurance company or other major lender, which put up 97 per cent of the money. Sometimes the promise of Enron stock would be put up to guarantee the loan, although Enron stockholders were never told of the risk that their shares could be diluted if such new shares had to be issued. To qualify as 'independent' from Enron for accounting purposes, a Special Purpose Vehicle had to be owned by someone else. So an outside entity would be brought in to make the required investment, perhaps a tiny percentage of the SPV's total start-up cash, sometimes illicitly lent by Enron itself. An employee told the *Houston Chronicle* (20 January 2002):

> Enron no longer owned the economic interest in the asset, but it did own control over it. In the sales contract with the vehicle, Enron promised always to act in the interest of the SPV. Lawyers and auditors said all this was OK.

> As the asset made money for the SPV—if it did, and many didn't—it made principal and interest payments to the lender and issued dividends to the outside equity partners, just like in a normal company.
>
> Enron got to report the proceeds of the sale of the asset as earnings. It had to repay the loan … but the debt didn't show up on Enron's financial statements.
>
> 'Investors don't like to hear you say, "Oh, I was wrong." So you start having a yard sale to boost CFO (cash flow from operations) and net income,' the employee said.

As the Enron indictments showed, there were plenty of accountants, bankers and lawyers as well as some senior management willing to participate in criminal or marginal operations. But they had nothing to do with any criminal subcultures as conventionally defined. Likewise, the many works on the savings and loans 'failures' (Black, 2005; Calavita and Pontell, 1993) and on accounting frauds (Tillman and Indergaard, 2005, 2007a, 2007b), which emphasize—sometimes over-emphasize—elite networks rather than socio-economically marginal firms (Shapiro, 1984), whereas there is no logical reason why both sets (plus 'full-time criminals') cannot be involved in frauds and money laundering.

Identity frauds and telemarketing scams

By contrast with notable criminal and 'close to the wind' entrepreneurs operating under their own personal names discussed above (though sometimes using many corporate and trust vehicles), other frauds may depend on false identities—wholly fictitious or 'borrowed' from real people—either for their commission or for the laundering process. Thus a senior executive or junior in the finance department might create a company or individual to receive payments, otherwise resting on their ability to make transfers without question: how elaborate the rest of the process is depends on how anxious they are to avoid suspicion and conviction. If the aim is to flee, then they may need false identities and that would usually involve others who can supply them consciously. If the aim is to stay and deceive, then it may involve others able to create a smokescreen of activities.

People other than insiders selling financial products need to find targets to approach and develop persuasive methods of getting them to part with funds. One way of doing so is to pretend to be someone else who is creditworthy. In the past, a simple method was to steal someone's credit card and (in the absence of photos on cards) look sufficiently plausible that a normally ill-motivated (in)capable guardian (in routine activities terminology) such as a shop assistant would sell goods to them or—a stiffer but still possible test—give them money at a bank counter. When Chip and PIN was introduced, this became much harder in the UK and in some terminals overseas, and the locus of fraud shifted to technological efforts to capture both, or to the use of cards and duplicate cards abroad, with UK-issued card

losses overseas doubling between 2006 and 2007, after remaining fairly stable or falling over the previous six years.[15] Chip and PIN necessitated a change in the organization of fraud to greater internationalization of conspirators: electronic details copied from cards (a particular speciality of Sri Lankans working in UK petrol stations) could be sent to confederates abroad.[16] Though this had happened before, it accelerated as a result of the improvement of protection against fraud on lost and stolen cards (Levi, 2008b). Likewise, the cruder forms of bankruptcy fraud in which new companies were created by people using false names and paid for the first few orders before accelerating credit massively, selling the goods off and disappearing, were frustrated by enhancements in commercial credit control and pattern analysis, necessitating either wider transnational frauds or 'less organized' frauds in the sense of fewer scammers operating in tandem (Levi, 2008a). A key point here is the interaction between changes in the technology and organization of crime prevention and changes in the levels and organization of fraud. (See McIntosh, 1971; for an influential early exercise along these lines.) Alternatively, 'identity thieves' can try to bypass the control systems by applying for new credit facilities in the names of their victims, using a variety of techniques to get around the change of address (easier in highly mobile societies like the US) or even diverting the victim's mail to their own address for a period. (See Copes and Vieraitis, 2007, 2008 for an interesting research study of identity theft: a more heterogeneous term than the phrase might suggest.)

Much of the 'criminal (auto)biography' literature is devoted to individual con artists whose lives—though highly entertaining (if one is not a victim) and glamorous (if one is wedded, as they mostly are, to the culture of consumption)—are not embedded in crime networks to any significant extent (see e.g. Forsyth and Castro, 2007; Redding and Abagnale, 2003). The seemingly endless biographies and ghosted autobiographies of the Kray brothers and their entourage focus on the violence and extortion rather than the frauds that helped sustain their London 'empire' in the 1960s. This applies also to the Jake Arnott fictional trilogy, where even The Long Firm—which from the title should be about bankruptcy frauds (Levi, 2008a)—is almost all about sex and violence. The main fraud work that focuses us on networks is David Maurer's classic anthropological book *The Big Con* (2000, originally 1940). There, the assistant grifters were drawn from the world of (white) professional thieves about whom Sutherland (1937) wrote, while the principals were specialist confidence men. Maurer describes evocatively the way in which the fraudsters set up their 'marks' (targets) in both short and long cons, and the sometimes elaborate storefronts they used for their scams (as seen in the movie The Sting, which was based on the book).

The contemporary equivalents of these are telemarketing fraudsters: 'boiler room' operators, who in one recent case (author interview with police) worked in a room with a tape continuously playing in the background to simulate a busy stock brokerage; and the '419' advance fee fraudsters who may hire or 'borrow' rooms when they know the legitimate users

are away to use as props in their stings. In some investment scams involving wines and spirits, or ostriches, the operators do have some real products on show, but vastly fewer than those 'purchased' by the victims.

How do they find their targets? This can be through random dialling of telephone directory entries; through share registers of public companies; through perusal of advertisements in personal columns, articles about wealthy people in the media; and through the use/purchase of existing 'sucker lists' (which, except for serial fraudsters reusing their old lists, is the only method that would require contact with other offenders). Shover et al. (2003) note that fraudulent firms employ sales agents who work from 'lead', or 'mooch', lists purchased from any of dozens of businesses that compile and sell information on consumer behaviour and preferences. My interviews with investigators in several countries (2008) suggest that exchanges of 'mooch lists' are extensive and rapid—once someone has subscribed to one lottery or other product by internet, post or telephone, they soon experience allied scam 'offers' from other fraudsters, suggesting that there is a sufficiently broad scope for fraudsters to be non-competitive.

Holtfreter et al. (2008) conducted an interesting study in Florida to examine whether low self-control was related to consumer fraud victimization. They distinguished between the targeting and actual victimization of the public and demonstrated that male consumers had a higher risk of being targeted (as in a previous case study of Ponzi investment fraud by Trahan et al., 2005), noting that since it is difficult for outsiders to judge whether people they do not know will engage in risky behaviour, demographic correlates or targeting are difficult to specify. They showed that fraud victimization was not a random event because, although the net may be cast at random, the financial behaviour of consumers was key. Traditional indicators of victimization such as going to bars at night were unrelated to fraud targeting and fraud victimization risk. So reducing financial risk-taking specifically might reduce the extent to which people with low self-control might become victims of fraud, though it would not have an impact on other forms of victimization risk. They conclude (2005: 209) that:

> Perpetrators choose potential victims based on obvious indicators of vulnerability …. Financial risk-taking … is not an easily recognizable manifestation of low self-control that fraudsters can observe and use to target potential victims. On the other hand, the routine activities of consumers such as remote purchasing methods, are detected more easily by perpetrators of fraud.

This leads to targeting of people irrespective of their levels of self-control.

How are telemarketing fraudsters organized? Some fraudulent telemarketing organizations consist of two or three persons who operate in a community for only a few days or weeks before moving on. These 'rip and tear' operators depend on the months-long lapse between the time they begin operating and the time law enforcement and consumer protection agencies become aware of and target them. Somewhat larger 'boiler rooms' feature

extensive telephone banks and large numbers of sales agents. Larger telemarketing operations commonly take on the characteristics of formal organizations, with hierarchies, a division of labour, graduated pay and advancement opportunities. Those who are ill-suited to cold call selling or who develop moral qualms simply leave the business.

In terms of 'scripts', if they wanted to commit a 'boiler room' fraud without being licensed, then all they would need is an office, a good telephone system and salespeople willing and able to persuade 'punters' to buy shares for more than they were worth. Unlike the cons described by Maurer—which are pure artifices and therefore must hire willing conspirators—the investment scams can hire junior personnel through advertisements and agencies who may be quite ignorant of the true rationale of the business. Only the originators may be active criminals. Some telephone salespeople may be experienced multi-scam participants (Stevenson, 1998; Shover et al., 2003, 2004), but others may simply have the (wilful or not) ethical blindness of commission-based income-generators: the sort of people responsible not just for telemarketing frauds but for financial services industry 'misselling' when working for major banks and insurance firms, leading to payments of hundreds of millions of pounds in compensation by the companies.[17] Some of those interviewed by Shover et al. (2003) had previous sales experience before beginning the work, but most did not: they either responded to ads in the newspaper or were recruited by acquaintances who boasted about the money they were making. Many were not succeeding at conventional careers, and telemarketing came along at a time when they needed to show that they could make something of themselves. They believed they were outstanding salespersons, who could sell over the telephone despite resistance from those they contacted; and they got a 'high' from doing so (see Katz, 1990; and Levi, 2008a for the emotional rewards from crime commission). These salespeople are unlikely to come from the 'general criminal classes' but rather from people with persuasive skills (some of whom may be 'shaken out' from financial services firms in recession), recruited by advertisement and via agencies, and incentivized by high commission and low basic pay. Such generic persuasion techniques are discussed by Cialdini (2007).

Shover et al. (2003) state that the sales agent generally works from a script that lays out successful sales approaches and responses. Promising contacts are turned over to a 'closer', a more experienced and better-paid sales agent. The hierarchy of the firms and the routine of turning prospects over to more experienced closers explain why victims typically report contact with multiple salespersons.

What factors influence the choice of venue for boiler rooms and their modus operandi? From UK cases examined, boiler rooms are commonly based abroad (e.g. in Spain, where police interest is low), never seek authorization by the Financial Services Authority (FSA)—which is a legal requirement to sell securities in the UK—and use high pressure sales and telephone

techniques (author interviews with UK officials and police). One more sophisticated technique is to approach a small UK company not listed on the Stock Exchange and propose to raise capital by selling £100,000 worth of shares in that company on their behalf. Of this £100,000, the boiler room would agree to take 60 per cent as its fee, leaving the small company with £40,000 capital. In reality, the boiler room will 'cold call' UK investors to sell the shares at up to 100 per cent over the agreed price, take their fee and vanish. The small companies involved may become liable to refund investors the full price paid for their shares. There are several variations on the method of committing the crime:

- complete con, where there are no shares in existence;
- different instruments used—stock, currency options (and even bull sperm);
- restricted (e.g. US 'Regulation S'), worthless or over-priced shares;
- purported involvement in raising capital for companies;
- market manipulation where there are shares in existence and a (limited) market;
- deceptive share promotion via bulletin boards.

If the fraudsters have sufficient nerve, they can seek to become regulated in one EU country and obtain a 'passport' to operate in another under EU single market regulations, using that as a base for fraud and making it difficult for local regulators to intervene to close them down. In all of these cases, what the boiler room is really selling is deceptive and worthless expectations.

The growth in cross-border consumer fraud operations can be illustrated by data from the US. (No equivalent data are yet available for the UK.) During the calendar year 2007, the US multi-agency Consumer Sentinel (which acts as a one-stop shop for complaints) received over 835,000 complaints—258,000 identity theft and 577,000 fraud-related complaints: the latter rose from 428,000 in 2006. Fifteen percent of the fraud-related complaints were cross-border fraud-related, down as a percentage (rather than as a number) from 23 per cent in 2006, reflecting the growth in fraud complaints rather than the number of cross-border cases.[18]

Foreign Money Offers was the leading product/service category in US consumers' cross-border complaints (12%), followed by Prizes/Sweepstakes/Gifts (11%), Shop-at-Home/Catalogue Sales (8%), Lotteries/Lottery Ticket Buying Clubs (7%), and Internet Auction (5%). Internet-related complaints comprised 59 per cent (50,907) of the total cross-border fraud complaints (86,074) received during calendar year 2007. To give some idea of the distribution of complaints (which includes reports from Australian, British and Canadian authorities), table 2 below tracks changes over time (Federal Trade Commission, 2008):

Although complaints about overseas businesses may not reflect nationality of the perpetrators, it may also illuminate to consider the amounts of money at stake ($194 million—around £100 million in 2007) see table 3,

Table 2. Cross-border fraud complaints by consumer and company location[a] (calendar years 2005–2007)

CY	*US consumers against companies located in Canada (%)*	*US consumers against companies located in other foreign countries (%)*	*Canadian consumers against companies located in the US (%)*	*Canadian consumers against companies located in other foreign countries (%)*	*Foreign consumers against companies located in the US or Canada (%)*
2005	21	64	5	4	6
2006	26	59	5	4	6
2007	21	62	6	5	6

Note: [a]Percentages are based on the total number of cross-border fraud complaints for each calendar year: CY-2005 = 87,193; CY-2006 = 97,034 and CY-2007 = 86,074.

from which should be deducted business costs to fraudsters. These may be fairly modest, even assuming they pay for their communications.

In a longer work it would be possible to draw parallels, in terms of the dynamics between setting and criminal act, in relation to a broader range of identity and other frauds: for example, application frauds and insurance frauds. If we take mortgage frauds, for example, fraud typically takes two forms: customers lying about their own means—i.e., exaggerating their income—and/or falsifying documents, such as creating fake payslips that show they earn an amount large enough to justify the mortgage they need, even if it is a multiple of their real income. This can be done simply by printing fake payslips, if necessary on a colour printer. Self-certificated mortgages (at higher interest rates) were allowed to cater for the increasing number of self-employed persons who could not produce genuine pay slips. (They might also include their 'off the books' income!) One incentive for mortgage introducers is that they are paid commission; one incentive for lenders is that they have sales targets to hit and performance bonuses to get, and non-payment usually comes much later. In some cases, the borrower is told there is no way they are going to get the mortgage they want with their income, and that they should leave that part of the mortgage application form blank. After they have gone, the broker inserts the false income. In the US particularly, there have been widespread scandals relating to commission-hungry brokers lying to purchasers about the affordability of mortgages, which they discover only when the initial low rates expire. In other cases, the would-be purchaser colludes with the broker. In other cases still, the broker (or lawyer) purchases the properties for themselves as beneficial owner, using the names and real or fictitious income details of clients. In a rising market, where there is demand (for example from students) for rental properties, fraudulent purchasers see little downside risk. In some cases,

Table 3. Fraud complaints and amount paid by US consumers against companies located in other foreign countries (calendar years 2005–2007)

CY	*Total no. of complaints*	*Complaints reporting amount paid*	*Percentage of complaints reporting amount paid*	*Amount paid reported*	*Average amount paid*	*Median amount paid*
2005	55,474	28,729	52	US$136,649,579	US$4757	US$1304
2006	57,644	50,471	88	US$142,457,801	US$2823	US$1050
2007	53,629	47,388	88	US$194,032,819	US$4095	US$750

valuers from a restricted panel are aware that the lenders need to lend and their judgment is swayed by this to give the valuation required to enable the mortgage to be granted: this is especially so where all the parties' desires are in the same direction (author interviews with surveyors, 1980s and 2008). However when the market turns, as it did in 2007 (and earlier in the US), these frauds are shaken out as people cannot keep up with repayments.

Ethnicity, nationality and the supply of offenders

The conventional way in which Organised Crime Situation Reports or their recent variant threat assessments have worked (see Edwards and Levi, this volume) has been to identify national or ethnic groups involved in serious crimes for gain. To some extent those chosen for this association reflect those groups law enforcement and intelligence agencies have access to, and are self-justifying in 'intelligence-led policing'.[19] Many national and religious groups have occupied places in the demonology of crime, but in the particular case of fraud, the two most common demons are Jews and Nigerians. Ichheiser (1944), reviewing the social psychology of anti-Semitism, argued that

> 'Gangsters' and 'swindlers' may be considered … as two *personified symbols* of … fundamental forms of danger in social life …. Especially, in times like our own, characterized by deep economic insecurities, ideological confusion, fluidity and impenetrability of intricate social processes, by propaganda, advertising, adulteration of goods, the man in the street feels himself far more deeply threatened by those rather 'invisible' social dangers than by overt coercion and violence. And he is getting more and more suspicious that those invisible processes by which he is threatened are intentionally, and for someone's advantage, manipulated by some kind of swindlers 'behind the scenes.' Consequently the swindler … *becomes the main symbol of the predominant fear*.

There is no need here to review the history of imagery that associated Jews with swindling, but it remains a much more restrained sub-text in the post-Hitler period, which understandably generates caution in its treatment in

criminological and media circles. I have made a decision here to include this aspect of 'the supply of fraudsters' to fraud networks because it is a popular financial services industry and law enforcement theme. Analysis of prosecution cases cannot but reflect any criteria that underlie the reporting, investigation and prosecution processes, and so factors in the above that protect social elites (such as those involved in Enron or in price-fixing cartels) might lead to their under-representation compared with social outsiders. Likewise, negative social stereotypes (for example about who 'dangerous criminals' are) that affected these processes will lead to over-representation.

The analysis of white-collar offenders in the US Federal courts by Weisburd et al. (1991)—using data largely drawn from the 1970s—showed that two thirds had no previous convictions but of those who had, only one in five had previously been convicted of white-collar crime. The ethnicity of offenders varies by offence type: anti-trust and securities offenders were 99 per cent white; but around a quarter of credit card fraud, mail fraud and bank embezzlers were non-white. Jews were significantly over-represented among securities offenders (though not compared with their numbers in the general securities industry); but not among other white-collar offences. Although the research on this issue has not been intensive, by inspection similar remarks might be made about the UK in the initial years of the Serious Fraud Office, but not subsequently. Thus all four convicted (but none of those acquitted) in the Guinness case (Levi, 1991) were Jewish in origin (though CEO Ernest Saunders had converted to Christianity). However overall, neither Jews nor Asians nor any other religious, ethnic or national group are significantly over-represented in UK SFO cases, taking account of their numbers in the corporate and financial services industries. Of course one needs no 'racial' theories about these connections, for they are often relationships of propinquity and mutual trust. By volume, most fraudsters are blue-collar rather than white-collar in background (Weisburd et al., 2001; Piquero and Benson, 2004), and some sub-sets of American offenders (for example 'identity fraudsters') are disproportionately black or Hispanic (Copes and Vieraitis, 2007). This merely reflects the fact that some types of fraud can be accomplished by 'ordinary' offenders, and there is a ready supply of willing offenders from poorer communities who would commit fraud if they had the technical and social skills required and the confidence to engage in such crimes. Whether many such persons would have the verbal skills to commit securities frauds—even 'boiler room' and suchlike that do not require formal qualifications—is more doubtful, but payment card and social security frauds are relatively low-skilled.

Discussions about 'fraud' with bankers in many parts of the world immediately throw up the word 'Nigerians' (author interviews; see also Peel, 2006 and Glenny, 2008). As with many areas of 'organized crime', international Diasporas have become a common focus of risk discourses, and Nigerians represent a nationality whose Diasporas—whether in Nigeria itself or in Australia, Ghana, Ireland, the Netherlands, North America,

Russia, South Africa or the UK (to mention only some countries where Nigerian fraud networks have been observed)—are more visibly active than most in the sphere of fraud. See also Aning, 2007; Smith, 2007 and United Nations, 2005. Peel (2006) has demonstrated that some areas and tribes are more likely than others to be involved in such frauds, and they tend to be loose confederations rather than a tight hierarchy of offenders. He notes (pp. 22–23) that fraudsters buy respectability and even adoration if they channel some of their money back to their impoverished home towns. As Mertonian strain theory might lead us to expect, locals recognize what they have gained while displaying little interest in how they have obtained it. The explanations for heavy involvement in financial crime of Igbo people from the country's east include

(1) The social and economic marginalization (and exclusion from government patronage) both before the 1967–70 civil war and since.
(2) Policing is particularly poor there and in Lagos and Delta state, which are also rich sources of financial crime.
(3) The east has the kind of entrepreneurial commercial centres around which this type of crime will tend to be found. In Northern Nigeria, by contrast, there is a much smaller private sector and more government-based corruption. In Yorubaland in the west, scams are often linked directly to the accounting, banking and legal professions, which traditionally attract many Yoruba.

One might add that from the point of view of the Nigerian people themselves, these 419 frauds are far less harmful than the networks of corruption and patronage among military and civilian leaders who—especially but far from exclusively under military dictatorships—have stolen billions of dollars of income from the Nigerian oil production and from contracts, and who have converted these funds for their own use: the so-called 'curse of oil'. Between the British police and the Nigerian Economic and Financial Crime Commission during the time of President Obasanjo,[20] four Nigerian state governors were charged with money laundering and/or fraud. But the 419s and other 'advance fee' scams—called because people, once hooked, usually become trapped into paying fees to advance the payment of 'their' money—are the 'outward-facing' side of Nigerian fraud and involve losses to Westerners.

More generally in cybercrimes for gain (including payment card fraud), though there are plenty of indigenous fraudsters in the UK and the US, Eastern Europeans have developed a reputation for technical skill and cross-border operations. There is nothing exclusive about these nationalities, but in identified American and British cases (which are only partly the product of what law enforcement choose to pursue), Lithuanians, Rumanians and Russians predominate in such forms of fraud, though Brazilians are playing an increasing role. Rumanians also have played a significant role in the use in the UK of technical devices on ATMs (such as the Lebanese Loop—first developed by Lebanese crime groups and now in decline due to technical prevention improvements) to capture payment card

PINs. However it is less obvious what the analytical value is of such ethnic and national identifiers, which unintentionally scapegoat large classes of individuals who may be largely innocent of involvement in crime.

Trahan et al. (2005) link fraud victim behaviour to 'the American dream', applying interestingly the more general criminological analysis of Messner and Rosenfeld (2001). Yet it is not obvious how specific to America this dream (or nightmare) is. Where people have some IT education and intelligence but few legitimate opportunities in their home areas, they often seek opportunities elsewhere. Especially given legal migration and employment controls (supplemented perhaps by discrimination)—or fewer good jobs available for anyone in their place of emigration than they expected—they may be tempted by offers from others seeking co-offenders or they may develop their own fraud schemes. This was what drove the emigration of (non-Jewish) Germans to London in the mid-19th century, whereupon some of them turned to bankruptcy fraud, often against German companies (Levi, 2008a). Thus it is unsurprising that irrespective of any prejudices among social control agencies, we get clusters of offenders with similar backgrounds: colour, language (which also shelters from surveillance), and geography (people sharing ethnicities, nationality and religion often live close to each other) all contribute.

Conclusion

Globalization of crime is part of contingent relationships between settings, with their rich and varied opportunities (reflecting patterns of business, consumer and investment activities), the abilities of would-be perpetrators to recognize and act on those opportunities (the 'crime scripts' perspective), and their interactions with controls, including law enforcement (touched only lightly upon here). Constructs of 'organized crime' should be (and are becoming) less obsessed with the structure of groups than with what people need from the largely illicit and largely licit worlds to go about the business of fraud. In other words, analysis of 'organized-ness' is becoming decentred and re-understood as much in terms of the settings in which offending and its precursors can take place as in terms of the acts themselves.

Such observations or claims about the contested and shifting nature of analysis over time complicate the already difficult question of whether fraud 'itself' has changed over the years. It seems reasonable to reflect on two 'historical' questions:

(1) In what respects has fraudulent activity changed, in terms of the sorts of techniques and organization that are or can be used, in relation to the efforts made (intentionally or not) to prevent frauds? And
(2) In what respects has the world of fraud changed and what would the sort of people with the sort of skill sets/networks who committed frauds in the 1960s and 1970s have contemplated doing today?

In relation to the first question, although the basic techniques used by fraudsters in the 1960s are still available today, especially against those investors and trade creditors who make only modest enquiries, the professionalization of investor protection and credit management in the UK, as well as consumer media interest, makes the commission of such frauds harder. E-commerce, the growth of lightweight, high value electronic products, and the technology of rapid delivery anywhere in the world have cut down decision times and opened up domestic and foreign markets to fraudsters within and outside the UK. At the high end of insolvency frauds, it seems doubtful whether the more skilful abuses of insolvency by those who, for example, establish beneficially owned corporate fronts offshore and then create artificial debts to them which enable them to vote in friendly liquidators or administrators, are any harder to commit or are any more likely to be punished today than they were 30 years ago. Formal social control—the police and criminal courts—has not been particularly interested in frauds other than the more visibly harmful 'widows and orphans' cases. There has been a growth in 'civil recovery' regimes, applying financial investigation and asset forfeiture (irrespective of criminal conviction) to supplement the post-conviction confiscation remedies that have replaced the Criminal Bankruptcy Orders. However even if they have substantial confiscatable savings rather than (as did the high-spending long-firm fraudsters interviewed by Levi, 2008 and the telemarketers interviewed by Shover et al., 2003, for example) spending 'their' proceeds as they went along, few fraudsters are high profile career criminals of a seriousness level that would interest the Serious and Organised Crime Agency. This question is connected to the second.

What forms of fraud constitute a 'rational choice' depends on the confidence, skills and contact set of any given individual offenders. The presence or absence of 'crime networks' known to and trusted by the willing offender makes a difference to 'crime capacitation': an issue often neglected in individualized explanations of involvement in crime. Choice of crime type might also be affected by age. Those offenders who were in their 50s and over might not be attracted towards the technological challenges of cyber-activities, and—except via close encounters on porn sites, in night clubs, or in prisons—the age gap might apply to co-criminality as it does to other features of contemporary life. So today's new generation fraudsters might gravitate towards more 'techie' forms of fraud, whereas if they were in late career, it might seem too risky to adapt in unfamiliar territory unless they could find someone younger to collaborate with. This is a general proposition about the relationship between age and risk-taking/innovation. Some fraudsters display a remarkable aptitude for creativity and constant testing out of commercial systems and private individuals for signs of weakness. This focus on 'criminal transferable skills'—the set of aptitudes including social networking individual/sets of offenders have—concentrates our attention on offender creativity, energy and social networking skills in finding co-offenders (or 'turning' non-offenders into co-offenders) and in

adapting techniques: many offenders (and non-offenders) lack one or all of these qualities.

Objectively, there are far more opportunities for disintermediated crime in late modernity than in the post-war decades. With only modest sophistication, the internet and social constructions of what is normal have made it easier for foreign natural and legal persons to defraud consumers and suppliers, for example via counterfeited or cloned payment cards. Fraudsters could be involved in the theft of personal data from garbage ('bin raiding') or by hacking into data storage facilities; or account manipulation by insiders, whether in call centres or elsewhere. (The offshoring of call centres led to periodic media alarm stories about blackmail and corruption in India: but it is nonsensical to think that this cannot happen in the UK, with badly paid staff and high turnover ratios. Indeed, there may be tougher regimes in Indian call centres—staff searches and prohibitions on mobile phones in the premises—than might be allowed in the UK.) Rings of staged accidents with claims for hard-to-falsify personal injuries would be within the skill set of some (once they worked out what to do), as would organized benefit fraud and—especially—the sale of counterfeit products, whose quality digital technology has done so much to improve, despite the best efforts of the anti-counterfeiting coalitions. For the more adventurous, scams can involve some currently fashionable musical or sporting events, or a social cause such as 'renewable energy'. One may expect some future scams involving carbon trading. The underlying concepts were available to investors at the time of the South Sea Bubble, but some investors in each subsequent generation and/or country have to learn the lessons for themselves. Arguably, as evidenced by declining savings ratios and the willingness to borrow against the legal security of homes in the UK and elsewhere, there has been a step change in people's expectations of steady state or rising affluence, and resistance to personal financial decline. When times get hard as they have done in the period 2007-09, people may take more risks to avoid downward socio-economic mobility, and this offers opportunities to fraudsters. At a policy level, this means that a focus on 'regulating' rather than 'eliminating' frauds is sensible: what constitutes an acceptable level of fraud may depend on who the victims are, how much they can afford to lose, and the collateral damage caused.

Notes

1 Professor of Criminology, Cardiff University. Contact details Levi@Cardiff.ac.uk. The author is grateful for the ESRC Professorial Fellowship RES-051–27–0208, under whose auspices this research was conducted. I also thank Nicholas Dorn for comments on an earlier version of this article.

2 Though one would not overstate the strength in depth of quality research on the organization of any crimes.

3 This is a technical neologism rather than the common language sense of 'script'.
4 There is an ongoing debate, which we bypass here, about terminology in the white-collar and corporate crime arenas (see e.g. Levi, 2008a). Financial crime (more commonly 'economic crime' in Europe) is a term broader than fraud, which also includes corruption and money-laundering.
5 Consider this in relation to the UK and the European National Intelligence Model, in which Level 1 refers to crimes within a police force area; Level 2 to crimes within the UK but involving more than one force area; and level 3 refers to international crimes. Does the mere fact that money is transferred overseas or credit cards are used fraudulently overseas make them level 3 crimes?
6 In some cases, they may encounter people (or companies) they consider to be potential suckers and then develop ways of fleecing them. There is a flexibility here that is poorly captured in the term 'organized crime'.
7 Rather than 'suspicious activities' or 'suspicious transactions', as is the official terminology, I consider it more analytically accurate to term them suspected transactions. Electronic transfers create a clearer audit trail if and when identified and followed than do cash movements.
8 I interviewed one offender who would have had difficulty in disposing of a truckload of yoghurt, had he not been arrested before he dealt with the dilemma. One 19th century fraudster obtained from Germany a gross (144) of artificial glass eyes which he was unable to sell and in the end, he had to dispose of for the price of the postage it cost to obtain them (Levi, 2008a).
9 The sanctions would have to be significant in terms of their own values in the 'communities' (if any) they inhabit. Cultural variations in legitimacy can be quite broad.
10 This echoes other practical failures in the fraud attempts of others, like taking too long a lunch break and therefore not being in the office when the bank rang to verify that the £25 million transfer request to a new account was intentional. These also give willing future offenders some useful tips to avoid!
11 Unless the purchases on 'borrowed' card data are picked up by the sophisticated electronic systems that model customer transaction patterns and contact customers proactively if there are transactions that do not fit their profiles.
12 The longer and more intensive an investigation, the more likely it is that surveillance will generate an accurate model of interactions between players in the network. Morselli and Roy correctly argue that when combined with an understanding of the roles that are hard to substitute, Social Network Analysis gives a better idea of the impact of enforcement interventions against central players. Sometimes one only learns impact after the operation/arrests, and in my view, one key question is whether in practice investigations do continue to test the disruptive effects: this might be hard to justify both legally (in terms of criteria for surveillance authorization) and financially (given severe constraints on police finances – someone has to be paid to listen, and this is especially expensive in foreign languages). Boundary assessments for determining the limits of social networks may be harder in fraud than in some other networks.

13 Though in some European countries, for example, people with criminal records are not allowed to become company directors.
14 This is not a recent issue. Lefkowitz (1963: 51) notes: 'In recent years, persons with criminal records have attempted by various guises to infiltrate the securities market, posing major problems for governmental regulatory agencies in the securities field. New York State has attempted by statute to eliminate persons with felony convictions from engaging in the securities business. Another problem in New York was high-pressure "boiler room" operations. A New York statute now requires registration of securities salesmen, in an effort to alleviate that problem. The gangster element has found it increasingly difficult to conduct business in New York under these enactments.'
15 Between 2000 and 2007, 'card not present' losses on UK-issued cards rose from £72.9 million to £290.5 million. In 2007, there were over 2 million 'card not present' frauds in England and Wales, a rise of 58 per cent by volume. However while the frauds of this kind quadrupled 2000–2007, online shopping increased tenfold to £34 billion. So the rise in fraud was modest compared with the growth in this form of consumer behaviour.
16 Hence some connection between payment card fraud and the financing of the Tamil Tigers (LTTE): but what proportion even of Sri Lankan card fraud went to finance terrorism rather than to sustain impoverished people or make some foreigners wealthy remains unknown—another example of the loose conceptualization of the link between organized crime and terrorism.
17 The distinction between mis-selling and fraud can be a fine one at times. The UK Financial Services Authority has set out criteria for judging mis-selling (http://www.fsa.gov.uk/pages/Library/Communication/PR/2003/052.shtml), stating 'it is the suitability of the recommendation for the consumer, not the investment performance of the product that matters. As long as suitability was established at the time of sale, and the required explanation of risk made, then consumer dissatisfaction about investment returns achieved gives no basis for an allegation of mis-selling. Investment performance may be relevant in assessing redress due where mis-selling is shown to have occurred.'
18 A fraud complaint is 'cross-border' if: (1) a US consumer complained about a company located in Canada or another foreign country; (2) a Canadian consumer complained about a company located in the US or another foreign country; or (3) a consumer from a foreign country (e.g. the UK or Australia) complained about a company located in the US or Canada. Company location is based on addresses reported by the complaining consumers and, thus, likely understates the number of cross-border complaints. In some instances the company address provided by the consumer actually may be a mail drop in the consumer's country rather than the physical location of the company in a foreign country, and in other cases, the consumer does not know whether the location is in the US or abroad.
19 'There is a well-justified fear that raids [by the UK Borders and Immigration Agency] have focused on ethnic minority businesses. The list provided on the Home Office website shows that 95% of those targeted

have been Indian, Bangladeshi, Chinese, Vietnamese and Turkish-run.' Such businesses are the easiest 'low hanging fruit' to fulfil organizational targets, compared with other workers in the hotel and food picking/production trades. (http://www.guardian.co.uk/commentisfree/2008/jul/16/humanrights.immigrationpolicy.)

20 After Obasanjo's departure from office, the head and then the acting head of the EFCC were replaced in 2008, suggesting to some the view of the new regime that they had become over-active in combating elites. Action against 419 fraudsters was more acceptable, since these were not usually connected to government elites (interviews with police and other officials, 2008). Despite the reputational damage 419 frauds and governmental corruption were causing to Nigeria, it seems unlikely that much of this policing activity in Nigeria would have taken place had the country not been 'blacklisted' by the Financial Action Task Force for inadequate anti-money laundering processes.

References

Aning; Kwesi (2007) 'Are there Emerging West African Criminal Networks? The Case of Ghana' *Global Crime* 8(3): 193–212.

Black, William (2005) *The Best Way to Rob a Bank is to Own One*. Austin, TX: University of Texas Press.

Block, Alan (1991) *Masters of Paradise: Organized Crime and the Internal Revenue Service in the Bahamas*. New Jersey: Transaction.

Block, Alan and Constance Weaver (2004) *All is Clouded by Desire*. New York: Praeger.

Calavita, Kitty and Henry Pontell (1993) 'Savings and Loan Fraud as Organized Crime: Toward a Conceptual Typology of Corporate Illegality', *Criminology* 31(4): 519–48.

Cialdini, Robert (2007) *Influence: the Psychology of Persuasion*, 2nd edn. New York: HarperCollins.

Copes, Heith and Lynne Vieraitis (2007) 'Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk'. Technical Report for National Institute of Justice. NCJ 219122. NIJ Grant No. 2005-IJ-CX-0012.

Copes, Heith and Lynne Vieraitis (2008) 'Stealing Identities: The Risks, Rewards and Strategies of Identity Theft', in Megan McNally and Graham Newman (eds). *Perspectives on Identity Theft*. New York: Criminal Justice Press.

Cornish, Derek (1994) 'The Procedural Analysis of Offending and its Relevance for Situational Prevention', in Ron Clarke (ed.), *Crime Prevention Studies*, vol. 3. Monsey, NY: Criminal Justice Press.

Cornish, Derek and Ron Clarke (2002) 'Analyzing Organized Crimes', in Alexis Piquero and Stephen Tibbetts (eds) *Rational Choice and Criminal Behaviour*. London: Routledge.

Cressey, Don (1955) *Other People's Money*. New York: Free Press.

Diih, Sorle (2005) *The Infiltration of the New York's Financial Market by Organised Crime: Pressures and Controls*, unpublished Ph.D. thesis, Cardiff University.

Federal Trade Commission (2008) Consumer Fraud and Identity Theft Complaint Data January–December 2007. Online: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2007.pdf.
Felson, Marcus (2002) *Crime and Everyday Life*. Thousand Oaks CA: Sage.
Felson, Marcus (2003) 'The Process of Co-offending', in Martha Smith and Derek Cornish (eds) *Theory for Practice in Situational Crime Prevention, Crime Prevention Studies* vol. 16, pp. 149– 67. Mounsey, NJ: Criminal Justice Press.
Felson, Marcus (2006) *Crime and Nature*, Thousand Oaks CA: Sage.
Forsyth, Neil and Castro, Elliott (2007) *Other People's Money: The Rise and Fall of Britain's Most Audacious Fraudster*. London: Sidgwick and Jackson.
Glenny, Misha (2008) *McMafia: Crime without Frontiers*. London: Random House.
Harding, Chris (2007) *Criminal Enterprise: Individuals, Organisations and Criminal Responsibility*. Cullompton: Willan.
Hertzog, Arthur (2003) *Vesco: From Wall Street to Castro's Cuba*. New York: Universe.
Holtfreter, Kristy, Michael Reisig and Travis Pratt (2008) 'Low self-Control, Routine Activities and Fraud Victimization', *Criminology* 46(1): 189–220.
Ichheiser, Gustav (1944) 'Fear of Violence and Fear of Fraud: With Some Remarks on the Social Psychology of Antisemitism', *Sociometry* 7(4): 376–83.
Katz, Jack (1990) *Seductions of Crime*. New York: Basic Books.
Leeson, Nick (1997) *Rogue Trader*. London: Time Warner.
Lefkowitz, Louis (1963) 'New York Criminal Infiltration of the Securities Industry', *The Annals of the American Academy of Political and Social Science* 347(1): 51–7.
Levi, Michael (1991) 'Sentencing white-collar Crime in the Dark? Reflections on the Guinness Four', *The Howard Journal of Criminal Justice* 30(4): 257–79.
Levi, Michael (2003) 'Organising and controlling payment card fraud: fraudsters and their operational environment', *Security Journal*, (16)2, pp. 21–30.
Levi, Michael (2008a) *The Phantom Capitalists: the Organisation and Control of Long-Firm Fraud*, 2nd edn. Aldershot: Ashgate.
Levi, Michael (2008b) 'Combating Identity and Other Forms of Payment Fraud in the UK: An Analytical History', in Megan McNally and Graham Newman (eds) *Perspectives on Identity Theft*. Monsey, NJ: Criminal Justice Press.
Levi, Michael, John Burrows, Matthew Fleming, and Matt Hopkins, with the assistance of Kent Matthews (2007) *The Nature, Extent and Economic Impact of Fraud in the UK*. London: Association of Chief Police Officers. Online: http://www.acpo.police.uk/asp/policies/Data/Fraud%20in%20the%20UK.pdf
Levi, Michael and John Burrows (2008) 'Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey', *British Journal of Criminology* 48(3): 293–318.
Levi, Michael and Peter Reuter (2006) 'Money Laundering', in Michael Tonry (ed.) *Crime and Justice: A Review of Research*, vol. 34, pp. 289–375. Chicago: Chicago University Press.
Levi, Michael and Peter Reuter (2008) 'Money Laundering', in Michael Tonry (ed.) *Handbook of Crime and Public Policy*. New York: Oxford University Press.

McIntosh, Mary (1971) 'Changes in the organisation of thieving', in Stan Cohen (ed.) *Images of Deviance*. London: Penguin.
Messner, Steven and Richard Rosenfield (2001) *Crime and the American Dream*. Belmont CA: Wadsworth.
Morselli, Carlo (2005) *Contacts, Opportunities and Criminal Enterprise*. Toronto: University of Toronto Press.
Morselli, Carlo and Julie Roy (2008) 'Brokerage Qualifications in Ringing Operations', *Criminology* 46(1): 71–98.
Passas, Nikos (2005) Informal Value Transfer Systems, Terrorism and Money Laundering. Online: http://www.ncjrs.org/pdffiles1/nij/grants/208301.pdf
Peel, Michael (2006) *Nigeria-Related Financial Crime and its Links with Britain*, London: Chatham House.
Piquero, Nicole Leeper and Michael Benson (2004) 'White-Collar Crime and Criminal Careers: Specifying a Trajectory of Punctuated Situational Offending', *Journal of Contemporary Criminal Justice* 20(2): 148–65.
Raw, Charles, Geoffrey Hodgson, and Bruce Page (1971) *Do You Sincerely Want to be Rich?*. New York: Viking.
Redding, Stan and Frank Abagnale (2003) *Catch Me If You Can: The True Story of a Real Fake*. London: Mainstream.
Shapiro, Susan (1984) *Wayward Capitalists*, New Haven: Yale University Press.
Shover, Neal, Glenn S. Coffey and Dick Hobbs (2003) 'Crime on the line: Telemarketing and the Changing Nature of Professional crime,' *British Journal of Criminology* 43(7): 489–505.
Shover, Neal, Glenn S. Coffey and Clinton R. Sanders (2004) [p4] 'Dialing for Dollars: Opportunities, Justifications, and Telemarketing Fraud', *Qualitative Sociology* 27(1): 59–75.
Smith, Daniel (2007) *A Culture of Corruption* Princeton, NJ: Prince University Press.
Stevenson, Robert (1998) *The Boiler Room and Other Telephone Sales Scams*. Urbana: University of Illinois Press.
Sutherland, Edwin (1937) *The Professional Thief*. Chicago: University of Chicago Press.
Tillman, Robert and Michael Indergaard (2005) *Pump and Dump: The Rancid Rules of the New Economy*. New Brunswick, NJ: Rutgers University Press.
Tillman, Robert and Michael Indergaard (2007a) 'Corporate Corruption in the New Economy,' in Henry Pontell and Gilbert Geis (eds) *International Handbook of White-Collar and Corporate Crime*. New York: Springer.
Tillman, Robert and Michael Indergaard (2007b) Control Overrides in Financial Statement Fraud, Report for the Institute of Fraud Prevention. Online: http://www.theifp.org/research%20grants/tillman%20final%20report_revised_mac-orginal-EDITED.pdf
Trahan, Adam, James Marquart and Janet Mullings (2005) 'Fraud and the American Dream: Towards an Understanding of Fraud Victimization', *Deviant Behavior* 26: 601–20.
Tremblay, Pierre (1993) 'Searching for Suitable co-offenders', in Ron Clarke and Marcus Elson (eds) *Routine Activity and Rational Choice*, Edison, NJ: Transaction.

United Nations (2005) Transnational Organized Crime in the West African Region, United Nations, New York.
Weisburd, David, Stanton Wheeler and Elin Waring (1991) *Crimes of the Middle Classes: White Collar Offenders in the Federal Courts*. Princeton: Yale University Press.
Weisburd, David, Elin Waring and Ellen Chayet (2001) *White-Collar Crime and Criminal Careers*. Cambridge: Cambridge University Press.

MICHAEL LEVI is Professor of Criminology at Cardiff University, School of Social Sciences.

Criminology & Criminal Justice

www.sagepublications.com
ISSN 1748–8958; Vol: 9(1): 119
DOI: 10.1177/1748895809102441

Erratum

Criminology & Criminal Justice 8(4)
Organized fraud and organizing frauds: Unpacking research on networks and organization
Original article DOI: 10.1177/1748895808096470

In this article, the author's affiliation on p. 389 should have appeared as Cardiff University, UK.

The author's biography on p. 419 should have appeared as follows:

DR. MICHAEL LEVI has been Professor of Criminology at Cardiff University since 1991. In 2007, he began a 3-year ESRC Professorial Fellowship (RES-051–27–0208) to develop research on financial crime networks, transnational economic and organised crimes and responses to them. Recent publications include *The Phantom Capitalists* (2008); 'Organised crime and terrorism', in *The Oxford Handbook of Criminology* (2007); 'Measuring the impact of fraud in the UK: a conceptual and empirical journey', *B. J. Crim.* (2008); and 'Suite revenge? The shaping of folk devils and moral panics about white-collar crimes', *B. J. Crim.* (2009).

SAGE would like to offer its apologies for publishing the errors corrected above.