White-Collar Crimes and the Fear of Crime: A Review

Michael Levi

Abstract The focus of this chapter is 'fear of crime' and – within severe data limitations and conceptual controversies – it interrogates the variations in fear of different forms of crime, white-collar and other. It begins by examining the state of 'fear of crime' policy and what we might mean by 'fear' in this sort of arena; goes on to review fears of and concerns about those white-collar crimes that have been researched; and ends with a discussion of their implications for thinking and policy about fear of crime generally and about what we can learn about it from studying fears about white-collar crimes. Despite real fears and even more real consequences of frauds, there is relatively little 'read across' between fear of white-collar and of many other crimes: the embeddedness of fraud in voluntary interactive routines seems to be accompanied by a lack of visceral reactions of 'stranger danger' fear within the general population, but the precise causal mechanisms remain unclear.

Introduction

This book as a whole confronts the extent to which explanations, patterns, and the control of 'crime' are generic or particular, either excluding or including white-collar crimes of various kinds; it also examines what white-collar criminology and mainstream criminology (without white-collar crimes) can learn from each other. The focus of this chapter is 'fear of crime' and – within severe data limitations and conceptual controversies – it interrogates the variations in fear of different forms of crime, white-collar and other. It begins by examining the state of 'fear of crime' policy and what we might mean by 'fear' in this sort of arena; goes on to review fears of and concerns about those white-collar crimes that have been researched; and ends with a discussion of their implications for thinking and policy about fear of crime generally and about what we can learn about it from studying fears about white-collar crimes.

M. Levi (✉)
Cardiff University, Wales, UK
e-mail: levi@cardiff.ac.uk

S.S. Simpson, D. Weisburd (eds.), *The Criminology of White-Collar Crime*,
DOI 10.1007/978-0-387-09502-8_5,

It seems appropriate at the beginning to highlight one important difference between fraud and other property crimes, and one that reduces very significantly the similarities between fear of fraud and fear of other crimes. With the exception of some 'stealth frauds' like the copying of data from credit cards and illegal electronic funds transfers, people hand over their property to fraudsters voluntarily, under the mistaken apprehension that they are transacting business – purchasing or selling goods, saving or investing or merely transferring funds – in their own interests. Thus, trust in business processes, in institutions and/or in people is a key element in fraud in a way that is absent from many burglaries, theft of and from vehicles, robberies, etc. Victim management in face-to-face situations may also be present in nonfraud offenses for gain – for example, robbery – and indeed, Sutherland (1937) stressed the importance of *social* skills in professional thefts in which victims and offenders meet. By no means all fraudsters meet their individual, corporate or governmental victims face to face. However, it is interesting to conduct a thought experiment on what we could do to manage a modern economy and survive old age if we were fearful that every transaction we undertook might be fraudulent.[1]

Fraud is, of course, present in other sorts of relationships that may give rise to crime. These include espionage (commercial or national/ideological), which arguably can be committed by psychologically 'normal' people, and other offences including white-collar ones that may be more likely committed by the sociopathic (Babiak and Hare, 2006). Manipulative behavior can occur not just for financial gain or espionage, but also for direct interpersonal or Internet-based 'grooming' of underage persons, and in adult relationships to gain opportunities for predatory date rape and violence within marriage. In such cases, success requires the initial nonevocation of fear or the disarming of suspicions. Our perception that we have more to fear from 'outsiders' whose aggressive intent or lack of self-control is manifest rather than from people we (physically) know and *seem* 'ok' makes us more vulnerable to manipulators: whether this perception is wholly socialized or is in any degree 'natural' remains moot, but victim cognition and conduct is important in facilitating fraud.

Fraudsters flourish where either we are not fearful of being deceived or the fraudsters have social engineering techniques that deceptively allay our fears. If the above conditions do not apply, then fraud could not happen outside of technological simulation which fools machines (such as the copying of magnetic stripe data and their re-encoding onto blank plastic) or our visual senses, like adulterated or counterfeit 'organic'/prepackaged foodstuffs, or car parts, whose authenticity we cannot judge by mere inspection. Paradoxically, the very fact that some fraudsters persuade us that we have lost money legitimately rather than fraudulently may reduce both 'fear of fraud' and the subjective impact of victimization among those who 'actually' have been defrauded.

---

[1] Or, for that matter, how we would function if we believed that every organization we dealt with might go into liquidation without compensation for creditors, even if it were managed honestly but unfortunately/incompetently.

Two important if all too often latent themes in 'fear of crime' are (i) what do our measures capture? and (ii) why do we judge the probabilities and impacts of different crimes in the way that we do? We can of course simply map out and contrast the levels of concern and fear about different crimes: but though interesting, this is not theoretically satisfying, as we often want to know how and why these arise. Fear, worry, and trust are concepts that are not just free floating or common sense, but are typified in three different theoretical traditions that apply to all offenses involving material or symbolic gain.[2] The Foucaultian tradition, following in the steps of the conflict theorists and also feminism, articulates *fear* and its management in the context of economic and ideological reasons (including the hegemony of masculinity and power). Weberians articulate the conditions under which rational calculation comes to the fore – impersonal organizations and markets – that include notions of personal responsibility and thus inevitably some degree of *worry* about the costs and benefits of different options for action. Durkheimians point to conditions for solidarity which are also the conditions for *trust*, basically the sense that we all belong to the same community: this is a mirage created and exploited by fraudsters, especially within close cultural or faith communities where pyramid selling and fraudulent investment schemes can easily spread. As the sorcerer *Comus* declaims in Milton's masque of that name:

> I, under fair pretence of friendly ends,
> And well-placed words of glozing courtesy,
> Baited with reasons not unplausible,
> Wind me into the easy-hearted man,
> And hug him into snares.

The Correlates of and Influences on Fear of Crimes

Terminology is important. It is appropriate to differentiate generalized concerns and worries from concrete 'fear' – defined in the Oxford English Dictionary online as, *inter alia*, 'The emotion of pain or uneasiness caused by the sense of impending danger, or by the prospect of some possible evil' and 'Apprehensive feeling towards anything regarded as a source of danger, or towards a person regarded as able to inflict injury or punishment' (see further, Gabriel and Greve, 2003; Jackson, 2004).

Fear is not necessarily based wholly on rationality. In a 'rational' world, one might expect (i) fear among nonvictims to be related to expected victimization risks and expected impact (which varies according to emotional/physical 'vulnerability'), and (ii) fear among crime victims to be related to these plus the actual impact of past experiences. (What the multiplier is empirically between expected risk/probability and expected impact, however, remains easier to theorize than to predict consistently.) Although most of us might want to avoid the things that cause

[2] I am grateful to Nicholas Dorn for this insight.

us fear, this is not always possible, since they may be embedded in our physical environment and be hard to escape, given our financial means and entitlements (e.g., to travel to safer environments).[3] Research excluding white-collar crimes indicates that personal crime victimization increases the fear of both personal and property crime, whereas property crime victimization only increases the fear of property crime (Rountree 1998). This might be a question applied to white-collar victimization, though this has not been investigated to date. Although their research predates '9/11' – which has transformed the security agenda via enhanced fears – the most serious crimes do not necessarily generate the highest fear (LaGrange and Ferraro 1987; Warr, 2001), perhaps because they are correctly seen to be less frequent.[4] Killias (1990) argues that fear is determined by three factors: *exposure* to nonnegligible risk; the ability to *control* exposure (protective measures and the ability to escape);[5] and the anticipation of how *serious the consequences* might be. However, in his analysis, control is seen in terms of vulnerability to physical attack. Are there any lessons here for fear of fraud? The equivalent in fraud might be the ability to control risks of identity invasion/take-over/card 'skimming'[6] (for individuals) or illicit qualifications/unauthorized financial transfers/credit control evasion for both staff and business functions (for business). One might further refine this to stress the importance of *perceptions* of the ability to control exposure, since we are not here predicting probabilities of victimization but rather fear of it.

We know comparatively little about the relationship between detailed exposure to the risk of victimization and fear, or its connection with lifestyles and routine activities. For example, if senior citizens (or women of whatever age) seldom go

[3] Consider the case of people living near toxic waste dumps in North America or in Bhopal, India (caused by environmental crimes); those living in public housing projects with very high crime rates; or in Darfur and other extremely risky spots without the right to travel to other countries. Of course, those embedded in a culture of masculinity and/or with particular sorts of personalities might seek out danger and challenges, so risk avoidance is far from universal. See Coates and Herbert (2008) for a research paper on the impact of testosterone and cortisol on stimulating risk-taking behavior that may lead to white-collar crimes: this may lead to victimization and/or to offending. In a sense, these are the opposite of fear.

[4] One might reasonably question whether levels of physical harm caused by terrorist attacks are higher than those from other violent crimes, from 'ordinary' homicides to health and safety at work violations and dangerous driving causing death: see Levi et al. (2007b). However, levels and forms of media representation and political action are very different. This serves to point up the difference between statistical risk and the phenomenology of 'the risk society'.

[5] Though a better way of thinking about this would be to recast it in terms of *perceptions* of the ability to control exposure, rather than the more objective measure of ability implied by Killias.

[6] 'Skimming' refers to the copying of information from the magnetic stripe on payment cards and their re-encoding onto other cards of varying degrees of realism, depending on the context in which they are used. In many parts of the world (especially Europe), skimming of domestic cards for domestic use is made pointless, since the cards work only when the microchip on the cards is activated by the correct PIN. In the United States, however, the economics of the card industry is different and the copying of magnetic stripe data on US-issued cards anywhere in the world is therefore profitable.

out much at night because of fear of crime (or so they say), it is not surprising that they are not mugged or raped by strangers very often; by contrast, young men who go out nightly are exposed to risk for much longer and much more frequently than their mere numbers would suggest. What are the analogies in the world of fraud? If people do not use the Internet (whether because of fear of fraud or anxiety about using technology), no 'phishermen'[7] can inveigle their online banking passwords, though they then cannot avail themselves of facilities and reduced prices that increasingly one can get only through the net. The importance of the electronic web to consumer and investment fraud can be overstated: avoiding it altogether still may not protect people from telemarketers' phone calls; from pyramid-selling webs whose rewards are based on recruiting friends into schemes; from local religious authority figures offering them 'unbeatable' returns on investments; from the regular impressive-looking letters informing them they have won the Spanish or some other lottery prize (even though they have never entered for it); or from the unwanted 'preapproved' personalized credit card offers that come through the mail but may not be shredded by recipients,[8] and thus may provide 'identity fraudsters' with good personal information that they can use for other credit applications, even if they do not make use of the offer directly.

Technically, a review of the link between fear and victimization might want to take into account the frequency of exposure to potential crime events rather than mere numbers per 100,000 population category: but such refined data are seldom available, for fraud or for any other offenses (and would be particularly difficult with cyber threats taken as an aggregate).[9] Paradoxically, as with people in high-crime areas who may be less fearful and even less often victimized than are strangers in those locations because they 'know their area,' frequent Internet users logically should be less susceptible to victimization from 'phishing' and other harmful e-mails, since if they get so many e-mails from banks where they do *not* hold accounts, they should be equally skeptical (fearful?) of those that appear to come from their bank. They also might actually read *and absorb* the warnings on their banks' websites that the bank *never* asks people online for passwords or confidential personal details. Such warnings are partly circumvented nowadays by fraudsters who have moved to 'vishing': they seek to allay suspicions by telling potential victims not to fill in security details online but rather to telephone the bank security department at a particular number, which happens to be their own fake bank telephone number rather than

[7] 'Phishing' means electronically simulating a legitimate business or government actor in order to persuade people to give their personal financial or other information. A common example is the e-mails that many of us receive telling us to update our security for a variety of online banks (at almost all of which we do not have accounts) or eBay.

[8] If they *are* responded to, this may contribute to the debt mountains, which have contributed to the subprime-related panics that led to major interest rate interventions by central banks in the United States and Europe, increasing 'moral hazard' by reducing the risks to imprudent lenders and borrowers alike.

[9] Imagine, for instance, that one were to look at payment card fraud risks per total number of times that cards were used, or even as a ratio of numbers of payment cards, rather than numbers of cardholders.

that of the target's actual bank. However, we know that some people are repeat victims of such scams (OFT, 2006; Titus and Gover, 2001), and that some citizens (disproportionately, senior ones) send a number of checks to fraudulent firms or throw good money after bad, like desperate gamblers trying to recoup their losses. Unlike the victims of repeat domestic violence or burglary, who may find it difficult to move and reduce their risks, these multiple fraud victims could say no and avoid victimization, but they are insufficiently fearful and/or have some personality that makes them vulnerable to repeat victimization.

To the extent that fear relates to perceptions of inability to control events, we might seek to differentiate fraud fears along those lines. Titus and Gover (2001: 135) helpfully divide personal frauds into those involving:

- 'No cooperation: A woman discovers in her monthly credit card statement that she has been the victim of an identity fraud, having done nothing to facilitate the crime.
- Some cooperation: A man responds to a "cold" phone call and contributes to a charity without investigating and learning that it was phony.
- Considerable cooperation: Having responded to an ad for a fabulous investment opportunity and been victimized in a Ponzi scam, a man is burned again in a recovery scam. Over a period of years, a woman loses many thousands of dollars in a series of one-in-five scams but continues to participate.'

The first may lead people to try to control risk by subscribing to account monitoring services; the second remains undetected and has a neutral effect unless the authorities learn about it from other sources and inform donors; the third may lead to the fearful avoiding victimization, provided they correctly identify the warning signs.[10] Australian research has found that older people who interact with their community feel safer than those who are isolated. Simply providing written information without social contact can sometimes increase levels of fear (James et al. 2003), but elderly consumers of fraud advice would need to be assured that those who are providing the information are acting legitimately.

Fear and the Media

An important link in the chain between actual risks of different crimes and fears thereof is the role of the media. Wall (2008) has examined the way that the media have shaped our images of 'cybercrimes.' However, the link between fear and exposure to crime stories is not clear cut. Otherwise, given the significant frequency with which fraud and corruption cases are reported in the 'quality' newspapers in the United Kingdom and (though researched less systematically) in the United States

[10] They may, of course, become ultracautious and see many 'false positive' indicators, in which case both they and the economy may suffer financially; on an alternative welfare model, they may 'buy local,' stimulating the local economy and arguably create more sense of community, benefiting them and others in their area.

(Levi, 2006, 2008), one might have expected fear of fraud to be quite high.[11] Nor is the reporting of white-collar crimes always unsensational. Ironically, though liberal UK media sometimes are very critical of some estimates of the terrorist threat, there seems to be little skepticism about high and rising 'cost of fraud' or 'cost of money laundering' figures; likewise with 'data' on some 'organized crimes' such as people trafficking. The extent to which such data increase people's (including business executives') fear of such crimes remains obscure, however. The link between risk and the 'actual' incidence/ prevalence of crime is also often obscured: thus a stolen business laptop with thousands or millions of people's financial or other personal data on it becomes massive 'identity theft,' and this in turn becomes 'identity fraud,' despite the often proportionately modest criminal usage of such data (personal interviews with industry and police). Parallels outside white-collar crimes would be the interchangeability in the media of 'Internet pornography' and 'pedophilia.'[12] These are part of a wider theme of the politics of fear (Gardner, 2008).

Skogan (1995) argued that the political genesis of 'fear of crime' during the late 1960s was stimulated by a 'fear of blacks,' fear of crime being an indirect way of expressing racial worries (see also, for the United Kingdom, Goodey, 1998, 2005). We will discuss later whether there are any parallels in the 'fear of white-collar crime' (or, since that category is itself highly diverse, of 'white-collar *crimes*'). However, illegal immigration has been an important theme in the coverage of 'organized crime' in the British media, and globally, Nigerians (and, in Francophone countries, Congolese) have come to 'stand for' fraud threats in the way that Jews once did in the European (and particularly Germanic) mindset.[13] Nevertheless, outside of Watergate

[11] An unexamined aspect of this issue is whether media stories principally tell us about 'just deserts' having been obtained or whether their motif is rather about crime existing/growing and being uncontained or unresolved. The former might be less fear inducing than the latter, though whether the dramaturgy and politics of 'law and order' ever allow that result is less clear. To the extent that – not least for defamation risk reasons – white-collar crime reporting takes place more after an arrest/raid/regulatory action has taken place than do events like violent assaults, then one might expect a larger proportion of frauds to be in the 'just deserts' category.

[12] To the extent that underage sexual portrayals involve real children and not artificial computer graphics, there is an undeniable connection between 'kiddie porn' and actual pedophilia: but given their numbers, it seems implausible that all such porn consumers directly commit offenses against underage persons. *A fortiori*, with adult sex fantasists.

[13] There is an older sociological 'fear of fraud' debate, exemplified in the work of those such as Ichheiser (1944) who were understandably absorbed by what underlay the social psychology of anti-Semitism. He 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.*

(now around four decades old), very few frauds or other 'white-collar' crimes constitute 'signal crimes' which evoke and symbolize wider problems in society, for example, whereby seemingly 'low-level' crimes such as graffiti are amplified into indicators of a wider lack of community spirit or social decay (Innes, 2004).

Politicians are distressed by the lack of impact of objective crime reduction on public fears or satisfaction with their crime-fighting performance, but it would be political suicide to suggest explicitly that voters are 'irrational.' Whereas risk management has become a routine activity of all business and public sector discourses (including the police, when allocating their own scarce resources), politicians seem locked into a model in which they cannot speak of or spell out an 'acceptable level of crime' – at least for any type of crime that the public/media care about – for fear of being portrayed as callous. This is doubtless one reason for the popularity of terms like 'zero tolerance policing' which have been transmitted across the Atlantic, despite limited evidence for their impact on crime levels (Jones and Newburn, 2006a, 2006b). When fear itself becomes defined as a significant cost of crime, and especially when media coverage is treated as a proxy for public sentiments, this has serious consequences for public policy and for cost-benefit analysis of crime control measures (for which, see Cohen, 2005). It is likely that people are more afraid of being stabbed or shot in the streets of London or Los Angeles than they are of dying as a result of industrial accidents precipitated by unsafe management practices, even though the statistical risks of death via the latter (and of course the risks of death on the roads by careless or dangerous driving) are higher: but despite the best efforts of 'corporate safety crime' and 'road safety' moral entrepreneurs, both media coverage and public fears do not reflect these differential rates. The implications of this for financial white-collar crimes of different kinds will be examined conceptually, though data are sparse.

Interestingly, although there are an increasing number of studies estimating (and, more often, wildly guesstimating) the direct economic costs of fraud, especially to business (see Levi et al., 2007a, and Levi, 2008, for a review), and these studies get well publicized via the efforts of PR agencies acting for the survey firms, frauds other than 'identity frauds' have been largely bypassed in the 'fear of crime' debate. This bypassing occurs both in developed and developing countries (e.g., in the International Crime Victimization Surveys, henceforth ICVS, and its regional offshoots), though the fact that the ICVS ask about consumer fraud and corruption – issues usually left out of developed country studies – reflects the importance of those crimes to people's consciousness in developing countries. Another way of looking at the absolute and relative salience of corruption to concern about 'crime' is the role that anticorruption campaigns play in elections, not just in developing countries but also in some EU countries like Poland.[14] But these appear to reflect anger at corruption more than they do fear of it.

[14] There is a broader debate we might have about the ambiguity of attitudes to corruption in places such as Italy and Louisiana. Perhaps in their mindsets, the fear of idle, rule-bound and incompetent bureaucracy unable to get anything done and of consequent economic decline is even greater than the concern about corruption? However, this is too large a topic for this essay.

Some fears – the fear of assault, for example – arguably are 'natural,' but even in those cases, perceptions of the incidence, prevalence, and even the effects of particular harms may be based on misinformation (Gardner, 2008) or even disinformation (i.e., the deliberate production of misleading information). The economic interests of individual and commercial security businesses cause them to amplify risks and/or present them in a sensational and geographically undifferentiated way, for example, 'there is one burglary every 40 seconds.' In other cases, perceptions of harm are shaped by media treatment, and these are affected by the way that the conduct is portrayed, either as events or in the aftermath of criminal or other official actions. Visibility, bureaucratic and commercial interests, ideology, and media production values and routines all play their part in media representations of both white-collar and other crimes. One of the principal differences – which also may affect and reflect the visceral emotions of fear – is that except for pure celebrity reportage, most white-collar crimes require more space and time for the story to be told and more concentration by readers and viewers to follow these stories than do other forms of crime; and that space is in very short supply in tabloid newspapers and television news.[15]

Levi (2006, 2008) notes that media coverage of financial frauds focuses on celebrity people and corporations (as offenders, victims and/or negligent storers of our personal data), 'widows and orphans' frauds against the especially vulnerable, cases involving dramatic harms or activities such as disappearance/discovery, and hi-tech crimes ('preferably' committed by juveniles or 'the Russian Mafiya'). All of these forms of offending do exist, but their salience is not as great among actual fraud risks as their media representation would suggest. The growing money and consumer sections of newspapers and radio/television programs frequently contain warnings about more ordinary scams such as Nigerian 'advance fee' and telemarketing ones. However the *effects* of media representations are often neglected by academics in favor of analyses of how the media portrayal is constructed and what economic interests it serves. Ditton et al. (2004) note that although there is an intuitively attractive connection between (a) media reports and dramatizations of crime and (b) peoples' fear of crime, an actual relationship between media and fear has been discovered surprisingly infrequently; their mixed methods study indicated that respondents' perceptions and interpretations of the media are more important than the frequency of media consumption and/or any objective characteristics of media material. In the context of white-collar crimes, this is likely to be the case also, to the extent that the public are exposed at all to particular types of white-collar crime.

Fear of Fraud Among Individuals – Some Evidence

What do we know about 'fear of fraud' among individuals? Unfortunately, the evidence is sparse on most forms of white-collar crime and in most countries. Fear of

[15] One could draw here some distinctions here about corporate health and safety crimes, where the physical events can be dramatically independent of the 'who is criminally responsible for this, if anyone?' question.

fraud (and, for that matter, actual fraud victimization) has until recently not been included in conventional criminological surveys in the United States, though the specialist and much smaller sample surveys by the National White-Collar Crime Center include questions on it, as do e-crime and the Pew Internet and American Lifestyles (2006, 2007) surveys. The Pew (2006) survey discusses senior citizens' use of and vulnerability to the Internet, while the Pew (2007) report discusses the nuanced reactions to spam: 'Spam has not become a significant deterrent to the use of email, as some observers speculated it might. . .But. . . 55% of email users say they have lost trust in email because of spam.' It is not clear what the implications are of loss of trust in this context, other than as an uncosted emotional impact. The US National Crime Victimization Survey (Baum, 2006, 2007) now contains some interesting questions on the economic and practical consequences of ID theft (very broadly defined), but does not address the psychological effects or the effects on future commercial actions, nor fear as commonly understood.

Krone and Johnson (2007) have usefully examined Australian perceptions of the riskiness of Internet shopping: two thirds of people with Internet access who had not used it to make purchases cited (in)security of providing credit card details over the net as the reason.[16] For reasons of space, the consumer fraud questions asked in the International Crime Victimisation Surveys do not explore the fear dimension at all. Likewise, in an already burdensome questionnaire, the questions asked in the British Crime Survey (BCS) since 2002 (see the valuable study of fear of payment card fraud by Semmens, 2003) are too few to explore the more subtle dimensions of fear; and it is symbolic for the marginalization of fraud that 'mainstream' Home Office publications regarding worry about crime have not discussed the data on card crime, leaving the latter to specialist reports on fraud and technology crimes.[17] Indeed, frauds against individuals and the fear thereof appear to have been 'technologized,' unconsciously neglecting the risks and concerns posed by more traditional forms of deception. Remote transactions are not the exclusive preserve of the Net; nor is the Net the only significant plausible source of anxiety about fraud. Thus, although their careful analysis shows that offline payment card victimization – though still much larger in total losses – has been falling as online purchases have been rising, Krone and Johnson (2007) fail to make the point that nearly all the Australian

[16] Of those who had used the net to buy things, 2% claimed more money had been taken than authorized; 3% that goods/services paid for were not received; and – more ambiguously – 4% that goods were not as advertised, in quality or quantity.

[17] The questions are

1. As far as you know, including anything we have already talked about, since the first of January xxxx has anyone used your credit card or bank card, or your card details, such as your PIN, to buy things or withdraw cash without your permission?
   Yes No
2. How worried are you about someone using your credit card or bank card details, such as your PIN, to buy things or withdraw cash without your permission?
   Very/fairly/not very/not at all worried/don't use cards

Internet crimes could have happened if the goods or services had been paid for by mail/telephone order rather than over the net.[18]

As for the perspectives of cardholders and the general public, Semmens' (2003) analysis of BCS data found that whilst worry about card fraud had many similarities with the other crimes at a descriptive level, it had a weak association with the other worries. Indeed those who are worried about personal crime are more likely to be worried about several crimes, or even crime generally. In contrast, those who are worried about property crime are less likely to have multiple worries. Worry about card fraud is generally not strongly associated with other worries but does have stronger associations with worry about mugging and attack. Worry about card fraud has the weakest total association with other worries. This suggests that worry about card fraud is quite independent from the other worries and may have different causes and correlates.

The 2002–2003 BCS (Allen et al., 2005) asked card users in England and Wales how worried they were about someone misusing their card or their card details in order to buy items or withdraw cash without their permission:

- Half (48%) of card users indicated a level of worry, with 15% stating that they were very worried and a further third (33%) fairly worried.
- A slightly higher proportion of women card users were worried than men, with 49% saying they were very or fairly worried compared to 46%.
- The proportion worried was lowest in the youngest (from 16 to 25) and oldest age groups (66 or over), compared to middle age groups (from 26 to 65).
- Black and Asian respondents were more likely than White respondents to worry about card fraud (61%, 67%, and 47% respectively).
- Levels of worry were similar regardless of education or social class.
- Those living in noncouncil areas were significantly more likely be very or fairly worried than were those living in council areas.
- Those who had been a victim in the past 12 months were significantly more likely than those users who had not been to be very or fairly worried about being victimized (68% and 47%, respectively). It appears that victimization may well serve to increase levels of anxiety, perhaps by exposing victims to the potential consequences of the crime.

People who used their payment card were asked whether they were worried about potential misuse of their cards or bank details in particular settings. The situation that caused most worry was buying goods over the Internet, with 54% of people who had used their card on the Internet being very or fairly worried about misuse in that context. The proportion of users of each of the other services had relatively similar worry levels, at just under half.

[18] Though readers should note that online purchasing has stimulated the growth of remote purchases, way beyond what would have happened if sales could occur only by phone or mail order after viewing products in catalogs or online.

In the 2003–2004 BCS (Wilson et al., 2006), over half (54%) of adults who had used the Internet said they had used a payment card in order to buy goods or services over it. This is a significant increase from 49% in the 2002/03 survey and may be expected to rise much further in future, as new generations appear who become accustomed to Internet purchases. Among Internet users who had *not* bought goods or services over the Internet, the most common reason given for not doing so was concern about security (72%); or worry about entering personal details online (37%). Despite reservations expressed earlier about the validity of identifying crime as the reason for avoiding activities, these seem grounded enough to be plausible. The noncrime issue of preferring to see the actual product before purchasing (22%) was another common concern. Those who did shop online were asked what precautions they took to secure their details on the Internet. The most popular precaution was to look for a secure site to buy from (73% mentioned this). Over a half said they only used well-known sites or companies (53% and 56% respectively) – though (not raised in the survey) the rise in 'pharming' and 'phishing'[19] with simulated websites might nullify this precaution as an effective prevention measure or even stimulate fraud by giving false reassurance. Unfortunately, there are no parallel findings for the United States or other jurisdictions.

According to the UK Financial Services Authority (FSA 2007)'s Financial Risk Outlook 2006, half of active Internet users were 'extremely' or 'very' concerned about the potential fraud risk of making an online transaction. Consumers who conduct their banking online are taking steps to protect themselves against fraud, by installing security software on their PC, but over a quarter do not know when they last updated their software or update it infrequently. Five percent of online bankers have no security software installed on their PC at all. The most common reasons cited are that it is too expensive, that they do not need it or they do not understand what it is. Many banks' terms and conditions reflect the voluntary UK Banking Code, whose current 2005 edition tells customers to use up-to-date antivirus and spyware software and a personal firewall (and some banks send antivirus software as well as other antifraud equipment free to their online banking customers). But the FSA found that nearly all users (95%) surveyed believe that at least some security responsibility should lie with the bank, while 45% believe banks should take sole responsibility (though there is no indication in the questions or answers about how the banks might do that).

Some intriguing data that may repay further critical exploration are contained in the survey of almost 1,400 people 18 or over reported by UK government campaign Get Safe Online (GSOL, 2006). To the question, 'Which of the following do you feel

[19] 'Pharming' is a hacker's attack aiming to redirect a website's traffic to another, bogus website. It can be conducted either by changing the host's file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers that resolve Internet names into their real addresses. 'Phishing' is a social engineering virtual attack to obtain user names and passwords that enable access to personal data.

most at risk from in your everyday life?'[20] Twenty-one percent (compared with 17% the previous year) stated that they felt most at risk from Internet crime, compared to 16% from burglary and 11% from mugging. For 27% (compared with an extraordinary 40% in 2005), bank card fraud was the crime they stated they felt most at risk from. Fifty-two percent of Internet users do their banking online, nearly a third (32%) pay their utility bills online and almost a quarter (23%) buy their groceries online. Half the public admitted to gaps in their knowledge about staying safe, and 76% of respondents felt that other people should have responsibility for their online safety. There is a significant portion of the population, though, whose fear of security breaches stops them conducting sensitive transactions online. Twenty-four percent of survey respondents had been deterred from online banking; 21% will not perform any financial management tasks online; 18% refuse to shop online and 17% will not use the Internet at all due to security fears (or so they respond). Though they may not add up to a very significant proportion of the total spend, the latter data are examples of fears that have economic consequences for financial institutions (and, perhaps, for the individuals themselves if they have to pay more for goods by purchasing only offline). However, the former do not measure fear at all, nor harm, but rather perceptions of riskiness. Nevertheless, the notion of fear of Internet crime does make sense, and this is a category that some people themselves use when describing their Internet-avoiding behavior.

Apart from surveys and interview based studies, one approach – the 'willingness to pay' model – might be to examine what products and services people are prepared to pay for in order to try to safeguard themselves or reduce (re)victimization. But quite apart from issues of affordability that hit the poor more heavily than the rich (who anyway can afford to self-insure), how do people make rational decisions based on knowledge rather than on rough guesses or even on disinformation by those seeking to make money from their fears? Direct retelling of actual victimization experiences can occur primarily only at a local level or through occupational networks (and then one must appreciate that many frauds against self and friends/colleagues are unknown to victims, since there are apparently innocent explanations for loss which fraudsters have deceived them into believing). Otherwise the media are an important source, but there are limits to the outreach of the regular warnings in both tabloid and broadsheet financial pages and on UK radio programs, and to the impact of such warnings on behavior. The UK Financial Services Authority and the Office of Fair Trading (and their Australian equivalents) have begun to follow US Federal agencies in communicating risk messages to investors in firms not covered by the Compensation Schemes (because the firms are not officially regulated). But the

[20] Unfortunately, these data were highlighted in box texts in the report and in the media coverage which, as so often, was drawn solely from the press release, as "People are more worried about criminals breaking in through their computer than they are about burglars breaking through their doors and windows" and "People fear internet crime more than burglary, mugging and car theft." This is typical of the constant elision between concern, fear, risk, and worry in the popular debate about crime. Analytically, it is far from clear that people would exclude Internet fraud when answering questions about bank card fraud.

extent to which these risk messages are read or taken notice of remains unassessed, at least publicly.

Nils Christie (2000) has drawn our attention to the role of the private sector, especially in North America, as a stimulator for profit of fear of street and household crime and of punitiveness: *inter alia*, these lead individuals and governments to purchase crime prevention technology, private policing and private prisons. In the twenty-first century, 'identity fraud' (often described as 'theft,' though the identity itself is mostly duplication or 'borrowing' rather than a pure zero-sum game) has become a particularly popular theme in the electronic and print media; in spite of guarantees by many card issuers to consumers against suffering losses from fraud when making Internet purchases, it appears to evoke significant levels of fear. This is enhanced by media coverage whenever large quantities of data are hacked or merely lost, as one may see from cases involving millions of people's data from the Veterans Administration (US, in 2006), TK Maxx (US and UK, in 2007), and HM Revenue & Customs (which in late 2007 lost in the normal mail unencrypted CDs containing the financial details of one third of the UK population!): in none of these cases was a significant proportion of the 'stolen' data *actually* used to commit fraud (interviews with the author), but the media/political row and the social anxiety continued notwithstanding. 'Awareness campaigns' are popular with vendors not just of physical security such as shredders – which have enjoyed significant rises in sales following publicity – but also of paid-for services such as account monitoring. There are annual 'Identity Theft' awareness weeks in the United Kingdom 'badged' by the Home Office but largely paid for by the industry, with local media events around the country. In addition to existing 'card fraud protection' bodies, which guaranteed compensation for card fraud losses that banks in the United Kingdom and United States are required to compensate anyway, paid-for services include 'fraud alerts' with credit reference agencies such as Experian and Equifax (plus Callcredit in the United Kingdom and TransUnion in the United States) that may tell you if someone has applied for credit in your name (but not, apparently, if they have used your US Social Security number with a different name); or indeed programs that hide one's IP address when going online.[21] There has indeed been criticism that suggests that like many forms of 'protection,' this constitutes secondary victimization by having people pay again for a service that offers very little more than what they could get for free or at best a partial, one-credit bureau service, compared with newer forms of ID fraud prevention and detection, some of which do limited credit monitoring but which keep an eye on other ID fraud windows by trawling Internet chat rooms and directories and by sifting through online public records for signs

[21] One such product, Zone Alarm's Anonymous Surfing, claims that it "protects you and your family from online identity theft by keeping your IP address (and your identity) private. It also protects you from visiting phishing, pharming, or spyware sites by displaying a warning notification of the hidden dangers ahead." Either this is an overstatement or it protects cybercriminals as well as potential victims. Many other products such as Internet Explorer 7 now offer phishing filters as defaults, in response both to consumer anxieties and objective risks: though objective risks by themselves do not create a market.

of Social Security number fraud, stolen credit card account trafficking, and other types of ID theft (http://www.consumerreports.org/cro/money/credit-loan/costly-credit-monitoring-services-offer-limited-fraud-protection-4-07/overview/0704_costly-credit-monitoring-services-offer-limited-fraud-protection_ov.htm?resultPageIndex=1&resultIndex=1&searchTerm=credit%20monitoring). Despite these limitations, Javelin Research and Consultancy estimates that some 24 million US consumers have paid $60–180 a year for these 'protection' services. (The number subscribing to equivalent services in the United Kingdom is unknown but also substantial: in addition, there are subscribers to Card Protection Programs which offer one-stop card cancellation services for cardholders plus largely unnecessary insurance against card fraud.) From November 1, 2007, all three major credit bureaus have made this protection available to all consumers in these states within the USA, even if they have not had their identities stolen.

In one-third of the several million cases of identity theft each year in the United States, 'stolen' (or, more accurately, illegally borrowed/duplicated) personal information like Social Security numbers are used to open new accounts in their victim's name. A security freeze gives consumers the choice to lock access to their credit file against anyone trying to open up a new account or to get new credit in their name. When a security freeze is in place at all three major credit bureaus, a would-be identity thief cannot open a new account because the potential creditor or seller of services will not be able to check the credit file. When the rightful consumer is applying for credit, he or she can lift the freeze temporarily using a PIN, so that legitimate applications for credit or services can be processed. For the 11 American states currently without security freeze laws, Experian, Equifax, and TransUnion will provide the freeze at no charge to identity theft victims and charge nonvictims $10 to initiate the freeze and $10 to lift it temporarily or remove it altogether (http://www.consumersunion.org/pub/core_financial_services/005085.html). A critical article in the New York Times (17 November 2007) asks the question why such freezes have taken so long and are so hard to implement: the answer surely lies in the profitability of these protection services, though one should add that the service provision is not cost free to the providers. Legislation mandating free security freezing thus costs the credit bureau owners something (though far less than the fees currently charged for implementing them).

These services are not offered free to British consumers, except occasionally in the aftermath of major private sector data losses or as part of some credit products. For an administration fee of £14.10 ($28) the UK not-for-profit fraud prevention service CIFAS offers a service, currently provided on their behalf by Equifax, to protect the name and address from identity fraud. People may contact Equifax, and request 'Protective Registration.' A CIFAS warning will then be placed against their address marked Category '0' which indicates the individual has been recorded on the CIFAS database at their own request for their protection. CIFAS members when undertaking a search against this address will see 'CIFAS-DO NOT REJECT-REFER FOR VALIDATION,' whatever name they search for. They will then contact Equifax to establish the reason for the entry. As a result of the entry CIFAS members will verify further the identity of applicants, and in some cases request from them further

proof of identification, and this may mean the citizens personally experience delays while their credentials are fully checked out. If people want to ensure the identity of a deceased person is not used by a fraudster to obtain credit or other products and services, a CIFAS Protective Registration may be placed by a relative or executor against the deceased person's address. Clearly the fact that people request this service and pay for it implies that they are afraid of fraud and the stress that resolving it generates.

Fear of crime and judgments about its probability and consequences might plausibly be viewed from the perspective of different participants, who may have very different levels of knowledge and experience, and may directly (as with bank financial crime directors) or indirectly (as contributors to Trusted Third Party industry-wide data bodies like CIFAS in the United Kingdom or to the liquidators/trustees of pyramid/securities fraud schemes) share their experiences to pool data as closed user groups (see Levi and Pithouse, forthcoming). In some cases, like CIFAS and the Insurance Fraud Bureau (in the United Kingdom), this fraud data sharing has a primarily preventative function, managing business risks collectively; in others, it serves less of a future crime-proofing function and more as a venue for communicating victim experiences and obtaining a share, however modest, in the payout from the assets of the defaulting firm or individual. There are also differences in offender and victim perspectives. As Semmens (2003: Chapter 7) acutely observes:

> The perpetrator of this kind of crime is simply using information, raw data, in the course of his/her criminal activities. By assuming control of information which does not 'belong' to him/her, s/he takes advantage of the pure instrumental value of the information. In contrast, the victim who loses control of the information attaches both instrumental and intrinsic value to that information and this impacts on the victim's identity. In short, the criminal act is simply the 'theft of identifying information' but the victim suffers 'theft of identity'.

The literature on fear of crime, especially violent crime, tends to focus upon the issue of 'stranger danger' and though violence-against-women analysts stress the analytical misguidedness of this, the general message that crime comes from 'without' remains strong and universal in different national research studies. Cross-national insights into fear of crime are underdeveloped in the literature. The rhetoric of globalization tends to underplay variations (Grabosky, this volume) – a point seldom made in television documentary or news programs that homogenize experiences or even in the criminological literature. However, when examining 'fear and risk of fraud' (and other crimes) comparatively, one should take into account national and regional differences in susceptibility, for example

- to have identities 'stolen' – for example, the far easier availability of identifiers such as Social Security numbers and criminal records in the United States compared with the United Kingdom;
- the clustering of people susceptible to fraud – for example, in 'gated communities' or favored retirement states such as Florida, which can be penetrated:

  (a) by remote telemarketers (Shover et al., 2003); or

(b) by face-to-face local or even national con artists pretending to be deeply religious people offering select chances to people of 'their' group. They, in a sense, succeed by disarming fears of strangers and expectations that fraud is committed by people who are 'not like us.' In faith communities, marketing is often 'viral' and all the more compelling because of this. It seems plausible that the willingness of respected people in our own communities to 'invest' acts as a trigger for others to follow, disarming fears and suspicions.

To some extent, these national and regional differences are becoming reduced via the use of social networking sites such as Facebook, MySpace, and Bebo. Data protection measures vary over time, but some such networking sites have data vulnerabilities that can be exploited by fraudsters and other criminals. As in many other areas, for example risks of violent victimization outside the home, young people may engage in risk-taking behavior and therefore, arguably, 'fail' to fear enough to protect themselves, for example, by putting online photographs and personal identifiers that can be used to build up composite pictures of themselves that make identity cloning easier. (Though they may also risk less because they appreciate that commonly used industry identifiers such as dates of birth and mother's maiden name are inherently weak and will be compromised.) However unsurprisingly, the networking firms themselves (including more business-oriented ones such as 'Linked-in') do not advertise their vulnerabilities, and whether risk knowledge reaches the kind of media that users see or hear *and take note of* remains uncertain.

Business and Fear of Crime

Fear is not a property one can readily impute to inanimate objects, so in strict terms, only business executives and their staff – not businesses themselves – can fear crime or worry about it. Several features of late modernity – in particular the requirements on financial services firms and professionals to report 'significant' frauds to financial services regulators and 'suspicious activities' (SARs) to Financial Intelligence Units (like FinCEN in the United States and the Serious Organized Crime Agency in the United Kingdom) – make total suppression of information about financial crimes practically more difficult and legally riskier than in the past. There is also more collaborative 'benchmarking' of fraud and money-laundering risks, though most such activities remain private and cooperation against fraud may be less common in countries such as the United States, where there is fear of regulatory/prosecutorial action for 'anticompetitive' behavior. Finally, one important difference between financial crimes and more conventional crimes is that the former break the normal *necessary* link of geographic propinquity between victim and offender that is logically necessary for involuntary asportation. Acts of corruption, fraud, product counterfeiting, and even consumer/worker safety violations may take place in different cities or countries from where the impact is felt. Whereas the normal construct of 'stranger danger' is of unacquainted offenders in one's locale, the fraudster could be a transnational offender posing as a local.

It is worth taking into account the economic externalities (costs) arising from risks and risk perceptions, not just in a domestic context but also internationally, an issue brought into sharper focus by events in Iraq and Russia in the early twenty-first century. Thus, 'business resilience' in the face of economic and political risk (including cybercrimes, extortion, and terrorism) has become a significant element in corporate risk management, and a substantial transnational private risk advisory and management sector has grown up to deal with such problems, to which a prelude is concern about, if not fear of, crime as one among many sources of business risk (Demos, 2006; Dorn and Levi, 2007, forthcoming; Gill, 2006).

One might add to this that insofar as retail businesses are located in areas perceived to be dangerous or risky by potential shoppers – an issue altered by e-tailing, which does not require physical proximity between vendors and purchasers – the risk judgments of those actual and potential shoppers also affect the level and time pattern of sales. Even ignoring the customers, however, one cannot make a neat division between fear of crime by businesspeople *in relation to their business activities* and the fear of crime by businesspeople and their employees *in relation to their personal lives*. Fear of being mugged or attacked for nonfinancial motives (including racial attacks) on the way to and from work, as well as – in the case of shopkeepers who live over the shop – fear of burglary, arson, or racial attacks are all relevant. Unfortunately, they are also under-researched.[22]

Many business crime risks and fears are only intermittently related to the area of corporate headquarter residence or to the residences of workers, and the globalization of retail and financial services create difficulties for these traditional constructs of space (Whimster, 1992), and for the physical space focus of the 'hot spots' literature. There is a paucity of survey as well as ethnographic data about business fear of crime, and what there is tends to focus upon the large retail sector and/or on fear of violence. However in principle, the issue of business and insecurity about crime in urban space can be represented in a number of different ways. First, in terms of the threats facing business, principally

- property crimes of different types (theft and fraud by outsiders, theft and fraud by insiders – perhaps collusively with outsiders – and criminal damage);
- violent crime (solely to cause hurt, without pecuniary motives); and
- both property and violent crime (i.e., robbery, which is *experienced* and feared as violent crime but has an economic instrumental purpose).

Second, in terms of the impact of this upon business and the community, for example, affecting business location decisions, including the flight from the inner city and estate blighted areas, with consequent effects on both employment and shopping (as well as crime) opportunities. (Fear of fraud seems unlikely to have such consequences, though experience/fear of corruption/extortion can drive businesses

[22] Ideally, one would like to see research on people who have left employment or self-employment, who have relocated or who have decided not to work in particular urban locations because of fear. However, such data are largely absent, except for the read-across from other research on fear and the city.

out of areas or countries.) Third, in terms of the concern of people at different layers of business organization, from blue-collar workers to senior directors: both their risks and their fears may be quite different, related partly to their economic interests and partly to their ability to purchase or otherwise receive security. Indeed, the term 'fear' should be treated with caution when dealing with a chain of command in a bureaucracy: front line workers and security staff working, living and/or traveling through 'rough' areas may have a very different cognitive approach to dangerous places than do their chauffeur driven finance directors/risk managers, commuting into corporate headquarters from homes in upscale areas. Fourth, about the crimes caused *by* business and the effects these can have, for example on consumer fraud, environmental damage, and health and safety at work. And finally, there are conceptual problems for the meaning of this subject area in relation to cyber crime risks arising in the course of rapidly rising e-tailing rather than face-to-face retailing. The importance of the 'new economy' may have been overstated, not least by those selling 'securities' (sic!) in the 'dot.com' bubble before 9/11, but e-tailing does extend further the disintermediation of the world of production from that of retailing and residence, envisaging customer delivery no longer from local or city center shops but rather from distant distribution centers, altering the shape of crime opportunities. Such vulnerabilities may arise at points close to consumers' residences (for example when fraudsters operate 'drop houses' for delivery of goods obtained by fraud or intercept goods before they are delivered to homes), but they may also arise close to points of distribution, when the loads are at their maximum.

The Fraud Problem and Business

Let us shift gear and focus for a moment on fraud as a social problem, and how it is dealt with. Where frauds – whether by or against otherwise legitimate business, or just outright scams against the public – do cause political concern, this tends to be generated by either hi-tech crime and/or by widespread investment and/or pension fund fraud, communicated via a substantial number of politicians; alternatively, in a sphere with parallels to violent crime, it involves some health risk to the public, such as contaminated meat products or dangerous counterfeit goods such as medicines or toys. Failures in supervision of the supply chain via globalized subcontracting – most recently involving China – may be the cause of or pretext for national alarms about product safety, fed by businesspeople and/or workers' representatives advocating protectionism in pursuit of their economic interests. (There is commonality here between countries as diverse as Australia, Russia, the United Kingdom, and the United States.) In other circumstances, fraud very seldom enters the core political agenda. The low fraud and business crime mail-bag content of ordinary politicians and government Ministers could be simply a reproduction of the lack of general awareness about whose business fraud is, since unlike 'normal' crimes, which are dealt with only by the police, frauds could be dealt with by multifarious bodies in the United Kingdom or North America. This confusion as to which agency(ies) people

might turn to is backed up by some research conducted by the Office of Fair Trading (2006) in the United Kingdom and by Kane and Wall (2006) for the United States.

If the allocation of responsibility for business crime enforcement seems complex, so too is the range of commercial bodies dealing with 'it.' It is appropriate to flag here the absence (with the possible exception of Intellectual Property) of a strong unified business lobby against all forms of fraud and other crimes which hurt business, though all business organizations campaign for legislative changes and enforcement action at a national and international level to support their economic interests. Since the criminal activities tend to be transnational, international bodies include the International Chamber of Commerce and the International AntiCounterfeiting Coalition, Inc. (IACC), a Washington, D.C.-based nonprofit organization formed in 1978. The IACC is comprised of a cross-section of business and industry – from autos, apparel, luxury goods, and pharmaceuticals, to food, software, and entertainment. The IACC's members' combined annual revenues exceed $650 billion. There are also sectoral trade bodies as well as individual firms that lobby for the protection of their interests.

Perhaps because 'fear' and 'worry' are seen to be properties of individuals rather than businesses,[23] there is an absence of research on which, if any, business sectors are *worried* about fraud, and this is a deficiency, since judgments about crime seriousness are far more abstract and reflective than are *fears* of crime: fear, after all, is an emotion. Nor are there any studies that explore the congruence or incongruence of fear, worry and crime seriousness judgments. This does not make survey findings meaningless – perhaps judgments about crime seriousness should be taken more seriously than measures that can largely reflect current media publicity campaigns? – but it does make them incomplete, by taking for granted the link between (a) thinking something serious, (b) taking personal or organizational measures against it, and (c) wanting something done about it by law enforcement as a priority.

Cyber Crime, Fears, and Risks

Moving away from areas such as violence (for entertainment and/or for financial gain, i.e., robbery) and burglary risks, which *require* – if not face-to-face in the case of burglary – at least some direct physical interaction between offender and victim (person or location), cyber fraud is disintermediated crime and there is a major question about where it and some other forms of commercial crime are to be located for both criminological and practical intervention purposes. For example, does the place where the crime takes place depend on where the offender is, where the victim(s) is (are), where the money is sent, where it ends up (properly laundered, or just hidden), or any combination thereof? These are not questions that arise in ordinary victimization or crime surveys, but they do have implications for fear of crime since the threats are more distant and less susceptible to normal policing

[23] Though media often report about the 'concerns of business' in other spheres affecting their interests.

methods.[24] To some extent the practical issues are taken care of by the shifting constructions of liability in criminal law. The Council of Europe Convention on Cybercrime 2001 (which came into force in 2004) aims to provide a common core to national legislation: the political support for it arises from the widespread fears of this highly dramatized area of crime. For example, in 'Internet sting lures 82,000 isle "lairds", *The Observer*, (10 March 1996) warned about a firm selling square-yard plots of remote crofting land to Americans with a fictitious scroll guaranteeing that for $100, purchasers will become 'an authentic Scottish laird.' The article began: 'In cyberspace no-one can hear the victim scream.'

A decade later, most Internet users have become habituated to receiving e-mails aimed at harvesting – 'phishing' and 'pharming' – data on their personal identities and financial transactions. In addition to dedicated identity fraud websites such as (in the United States) http://www.ftc.gov/bcp/edu/microsites/idtheft/, the regular flow of media stories in the West is part of the general advisory role of the media, but it also reflects the alarmist technophobia that is prevalent whenever risks of new technology are exposed (see also Mann and Sutton, 1998; Grabosky and Smith, 1998; Levi, 2001, 2006; Wall, 2008). In media terms, for *any* type of crime, subject to the (variable) need to be or to appear to be socially responsible, a 'good prog[ram]' is one that alarms the public and attacks the competence of large institutions, in this case their competence to hold our data securely.

This technological risk theme has been re-iterated frequently in trade and general media coverage of credit card Internet transactions, and may be one reason why surveys find considerable anxiety about Internet fraud risks among the general public as well as among retailers. My interviews with major credit card payments systems security heads indicate a unanimous view that fear of being defrauded inhibits commerce substantially, though no work has been done on examining the extent to which this fear relates specifically to factors such as hacker interception or fraud *by* merchants, nor has the opportunity cost of these losses to consumers and to business been quantified. E-tailers normally have to pay all the costs when they are defrauded, even though credit card companies usually absorb the cost of fraud for offline retailers. What has happened has been a two-pronged response, with (1) some card issuers offering consumers a fraud risk guarantee – which is a low-cost option since, unknown to many cardholders, they are liable anyway for a maximum of $50 in the United Kingdom and low amounts in many other countries – and (2) e-tailers and others selling goods over the phone being offered access to the true addresses of cardholders so that if they want to supply to addresses other than the home address, they know that they are taking a risk (about which they might be concerned, if not fearful). Business surveys are repeated quite regularly, for example by CyberSource and by Javelin Strategy and and Research (2007), which reported a fall in identity

[24] The distinction between telephone and cyberstalking is far less than that between physical stalking, but all types can occur to businesspeople as well as to individuals. Legal jurisdiction over cyberspace is a particular issue with cybercrime, whose legal venue is particularly problematic, as was discovered when the Philippine authorities released the suspected author of the Love Bug virus because their legislation did not cover it.

fraud the previous year. There are also broader e-crime annual reports in the United States by the Computer Security Institute (2007 – the 12th survey), in collaboration with the FBI, that generate substantial publicity but (other than in ritual introductory remarks) ignore serious problems in response rates and sample frames in a repeat cross-sectional study with an unknown number of repeat respondents rather than the panel study that would indicate far more about trends.

At the *individual* level, there are modest amounts of data, which may reflect as well as stimulate media coverage. Thus reporting on the British Crime Survey, Wilson et al. (2006) note that around 3% of the population were victims of check and payment card fraud in 2003–2004; half of the four fifths of respondents who had used a credit or debit card in the last 12 months were worried (including fairly or very worried) about being a victim of card fraud. Fifteen percent of individuals were very worried about being a victim of credit card fraud: this is similar to levels of worry for car crime and violent crime (15% and 16% respectively) but slightly higher than burglary (13%). Individuals were slightly more likely to be worried about card fraud when they were using their cards to buy goods over the Internet or over the phone (in both cases 52% were very or fairly worried about this). Overall the level of worry rose only modestly compared to 2002/03 (when it was 48%), and – perhaps because the fearful were less likely to buy goods online – slightly fewer who had used their cards to buy goods over the Internet were worried (55% in 2002/03 to 52% in 2003/04). However, one might question whether statements about levels of 'worry' properly reflect people's estimations of the impact that crimes are likely to have on them if they occur (i.e., they relate more to perceived probability than to perceived consequences). Since then, the United Kingdom (though not the United States) has introduced cards with microchips that require a PIN, so despite regular media reports on identity thefts involving cards (most dramatically the 47 million UK and North American cardholders whose data held by retailers TK Maxx were compromised in 2006–2007), the next set of data should be interesting, since Chip and PIN does not affect the Internet and other card not present risks, but has led to a significant fall in frauds on lost and stolen cards (APACS, 2007). Here, again we see the tension between data-informed and mediatized fear of crime.

Though media 'panics' about crimes have become routinized in contemporary society, it is plausible that 'identity fraud' and 'identity theft' – whose parameters are obscure – have indeed become 'signal crimes' that are treated as symbolic of the way in which technology has rendered us defenseless to preserve our unique selves. A report by business intelligence/credit reference agency Experian (2007) notes, with an appropriate degree of statistical caution:

> The rate at which new victims are contacting Experian continues to grow. 2,124 victims contacted Experian's Victims of Fraud team for the first time in the second half of 2006. This compares with 1,478 for the same months in 2005, and 926 in 2004, and represents a 69 per cent year-on-year increase in identity fraud activity reported to Experian. While some of the increase in number of victims contacting Experian could be attributed to increased awareness of identity fraud, rather than an absolute increase in victims, it is more likely a combination of both. . . . .This evidence of the growth in identity fraud activity echoes figures from CIFAS as well as from Experian's own fraud prevention business. CIFAS figures show that the number of victims of impersonation rose by 34 per cent between

> 2004 and 2006, while the number of fraudulent applications detected by Experian's fraud prevention systems for mortgages, loans, credit cards and other finance and leasing was 25 per cent higher in the second half of 2006 than the first.

However, its press notice was understandably sharper in tone, and all of the media simply reported the 'fact' that identity fraud had risen 69%: the headline, for example, on the front page of London's free Metro newspaper and a major news item in most other newspapers and television (12 April 2007). Experian advertises its free check of credit ratings and requests for credit on its CreditExpert product (though people who sign up for the free service have to agree to pay from one month later, which will be charged unless they remember to cancel!).

This is not to say that there is no deconstruction of fraud risk data. In the United Kingdom, there are prominent people such as Ross Anderson, Professor of Computing at Cambridge University who frequently debunk banking industry statements about security and appear on radio and television; and critics – on both ideological and pragmatic grounds – of the UK government's identity card proposals (www.no2id.net/), who regularly discredit the links between crime and the expensive 'solutions' offered. Privacy advocacy in the United States is also powerful compared with the United Kingdom, though eroded significantly since '9/11.' The consumer movement in the United States has also been more active in relation to identity theft, possibly because of a greater volume of such behavior and poorer general privacy in the United States than in the United Kingdom and Europe as a whole.

Setting aside all the hype, there is a serious social point about the interaction between computers, trust and security. As Grabosky and Smith (1998: 47) put it,

> [T]rust and confidence in the systems that support commerce, communications, air traffic control, electric power generation and other modern institutions are at the very core of our society. Thus, even the potential for disruption and harm is cause for concern.

The difficulty with this National Security perspective on cyber crime – which has become even more pronounced since the Love Bug virus and since '9/11' and subsequent use of the Internet by terrorist networks – is that if social harm is so seamless, what may *not* be affected by such risks and what are the limits of state intervention to prevent them from materializing? Furthermore, though this may affect the large corporate sector rather than the small owner-managed businesses to be found in the poorer areas of the city who may be more worried about transparency to the Internal Revenue Service than to intelligence agencies, is the fear of crime outweighed by concern about invasion of privacy on the part of intelligence agencies seeking to combat organized and/or political crime[25]?

---

[25] or seeking the economic preferment of their own national companies by governmental espionage in the late modern form of what General/President Eisenhower once termed the 'military industrial complex.' French businesses have alleged the misuse of electronic interception to win contracts for American companies, though this is hotly denied by the Americans and British. The irony here is that in the views of many Anglo-Americans, the French have been enthusiastic in their use of corruption to assist their own sales, so even if this had happened, it might merely counterbalance the illicit benefits to French multinationals from transnational corruption.

Fear of Fraud and Fear of Loss: A Problematization

Fear of crime – any crime – is a more difficult construct than might appear, and its application to white-collar crimes is at times tenuous. There is for all crimes a danger that the objects of fear may be mistaken – whether from racist socialization, media projections or other sources. Our exaggerated estimates of the risk of 'stranger danger' and our underestimation of 'male family danger' are a case in point. In relation to fraud, it is easy to see how such emotions of fear might arise from the perception that the drugs one was taking for malaria or HIV might be inactive counterfeits, or the car/airplane parts might be unsafe fakes. With some imagination, the prospective collapse of a retirement fund invested heavily in Enron or a bankrupt insurance company might also fit within that framework. These are dangers and/or evils, and at an abstract level may be recognized as such. It is also hard to tell whether such risks are present or not: the physical characteristics of goods or investment products do not enable the inexpert to tell whether or not they do what they claim – this is especially true of longer term investment products, whose benefits may (or may not) materialize in the distant future. Claims of expertise are hard to verify or falsify in advance. Hence the panic that sets in when people think 'their' bank or other vehicle holding their life savings *may* go bust.

zHowever the specific *fraud* component of such fears is harder to identify, as fraud is just one possible cause of economic catastrophe, or – at a more aggregate level – of what economists term systemic risk. Indeed, the 'credit crunch' of 2008–2009 triggered by excessive subprime loans shows us what happens when banks do not trust each other's ability to repay loans: however for the most part, this is bankers' fear of bank insolvency rather than fear of the banks committing fraud. Thus, during September 2007, television screens and newspapers in the United Kingdom (and – more rarely – even in some other developed countries like the United States) were treated to pictures of lengthy queues outside Northern Rock Bank branches in parts of the United Kingdom to withdraw savings, as people showed their fear of losing money due to possible bank insolvency. Their fears were stimulated by the news pictures, and the panic occurred despite the reassuring words of the Chairman of the Northern Rock, the Chairman of the Financial Services Authority and the Governor of the Bank of England: unlike the United States , where financial institution failures have been more commonplace (and deposit insurance more generous and quicker to pay out), it was the first run on an authorized UK bank since that on Overend Gurney in 1866.[26] The fear of burglary or robbery of the cash

[26] Overend Gurney & Company collapsed in 1866 owing about $20 million (at historic prices – around $11 billion today). Unlike Northern Rock, it was not a retail but a wholesale bank second in size only to the Bank of England, lending to other banks and finance houses at higher rates of interest: the day after it suspended payments, panic spread across the City of London, with large crowds waiting around its City offices and it had to be liquidated. The financial crisis following the collapse saw the Bank of England base interest rate rise significantly and over 200 companies, including other banks, failed as a result. Overend Gurney's financial adviser was jailed but the bank directors were acquitted on the grounds that they had merely made errors of judgment. The Gurney family was one of the most respected banking dynasties in England and their family bank

withdrawn from those 'hot spots' must have seemed far less salient to depositors – at least at that moment – than the prospective failure of the bank. This was even though deposits up to $70,000 – a third of the United States guarantee limit – were protected by a compensation fund. One regulator told me that one depositor tried to take out almost $2 million in *cash* from his account, somehow expecting that the branch would have that much in its tills – a cashier's check might have been safer and easier to transport, but not as reassuring! The government had to lend the bank $50 billion to stabilize it and in February 2008, it took Northern Rock into public ownership because the deterioration in availability and cost of wholesale market funds made it unviable, and private sector bidders did not offer a worthwhile alternative. At that point, fears of insolvency disappeared and savers flooded back for the high interest rates in a context of an unlimited government guarantee.

This wholesale loan market shortage for international and local banks arising from the United States subprime credit crisis generated immense anxiety in the United Kingdom, irrespective of the allegations that dishonest mortgage brokers conspired with them (though to a lesser extent than in the United States) to falsify their self-certificated incomes. Indeed it is not clear what the effects of such frauds (or beliefs that fraud was involved) were on the fears and anxieties of American or British savers compared with fears about their 'mere' inability to pay mortgages and their economic futures. Rather, labeling the acts 'fraud' may be a way of (unconsciously) enabling people to feel more comfortable with the fact of loss, diverting self-blame and expectations of low regard by others for 'unwise' savings strategies. In the case of Northern Rock, though fraud might have provoked greater anger among the public, the huge potential costs to British taxpayers of the support were almost independent of any issue of criminality. Fraud might even have given greater possibility of loss recovery from banks and lawyers who might have been held negligent.

Likewise, in relation to the much-discussed US Savings and Loans crisis during the 1980s (e.g., Black, 2005), to what extent were anxieties or even perceptions of wrongfulness the result of fraud by executives rather than simply economic loss compensated ultimately by the taxpayers? In the United States , in the aftermath of the collapse of the subprime market in 2007, there were allegations (interviews with officials and, for example, http://www.nytimes.com/2007/09/09/business/09every.html) that in order to obtain commission from the lenders, mortgage brokers (i) lied to unsophisticated and mostly poor people about the interest rates and other conditions of their loans as well as (ii) helped them lie about their incomes in order to get mortgages. Investigations of such allegations led to widespread FBI raids in 2008. However, although those people may be (rightly) fearful about their futures and may objectively be worse off than if they had not bought a home at all, whether this distress constitutes fear of *crime* remains more doubtful. In a sense, if they had

in East Anglia was unscathed: they became founding partners in Barclays Bank 30 years later. For a broader discussion of fraud in the Victorian era, see Wilson (2006). In 2008, bankers were reluctant to lend to other bankers not because they feared fraud but because they feared that the counterparty would not be able to repay them when debts fell due.

been more fearful of their brokers, they might not have become (a) victims of poor investments and (b) arguably, both fraud victims and fraud offenders. (The fact that brokers may have advised them on how to lie about their income when filling in their mortgage forms does not make clients innocent of obtaining loans by fraud.)

Unlike the S & L crisis of the 1970s – where the vast multi-billion dollar direct losses (only some clearly attributable to fraud) were confined to the United States – the losses from subprimes were also globalized through the sale to international financial institutions of Collateralized Debt Obligations rolling up large numbers of mortgages into a 'security' (sic!). However here again, fear of economic and status loss is not the same as fear of fraud. If bankers had been more fearful that what they were buying was overpriced, the market for these securitized loans would have been thinner and the economic damage less: though this assumes optimistically that bankers' respect for institutional and investor interests would have been greater than their personal greed for short-term bonuses. The human capacity for rationalization of self-interest in such circumstances is profound, especially if retribution is not anticipated.

Conclusions

It has proven difficult to demonstrate what students of 'fear of crime' can learn from the literature on fear of white-collar crime, and vice versa. This is partly because they are different sorts of activities that are often committed by different sorts of people, though there is an under-researched overlap in those who are offenders or victims of both. White-collar offenders purposively manipulate fear by trying to lower it, in circumstances where distrust exists; while fear of crime arguably is a consequence of street-crime victimization and the way in which information about it is constructed and disseminated. The closest to fear of street crime is fear of identity theft, which merges also into our fears about computers and our own loss of control over our 'selves.'

The parallels that are closest to the more general themes of this book are those involving the social construction of fear. Western nations tend to assume that what is bad for business is bad for society, but whether or not one accepts that general proposition, in both policy and theoretical terms, it is important to tease out the range of interests that are being promoted. Except as part of some corporate policy and image development strategy, businesses are primarily interested in the ways in which crime and concern about it on the part of customers, employees and owners affect trade volumes, profit and the cost of capital. Except where it has a reputational effect on the entire business – as *at some currently unknown level of perceived* frequency, e-commerce fraud and insider trading may – neither businesspeople nor law enforcement are especially concerned about fraud *by* businesspeople (though many frauds are by business against business, so it would be mistaken to see this simply in terms of 'class' or group interests). The public normally have little option other than to trust the products they buy: they may have particular insecurities about being sold

things by doorstep or by telephone salespeople, but presumably this is not universal or those activities would be unprofitable. Fear – in such contexts – is unproductive because there are no practical steps that one can take other than to withdraw from the market.[27] (Though in the case of Internet sites, they may take their revenge by blackening the reputation of the vendor; or only use one particular credit card for all their Internet purchases, avoiding – by not using a debit card – the risk of having their bank account emptied.)

Whereas fears of some crimes may narrow down opportunities but can seldom provide total protection from predatory attacks, fear of fraud might lead us to choose arenas of saving and investment that are wholly protected by government or insurance-based compensation schemes. To that extent, it may be a tautology that the absence of (or submergence of) fear is a precondition for fraud. Shapiro's (1990) classic article on 'collaring the crime, not the criminal' argued that the key to white-collar crime was the separation between agent and principal, the implication being that in a modern economy it was impractical fully to negate the risk of fraud. However, subject to maxima fixed by law in compensation schemes and the ability to recover assets in excess of this from the offenders themselves, fraud risks can be mitigated and therefore fear rationally reduced in some areas of life such as financial services/pensions schemes. However it is less plausible that evasive action arising from fear of fraud can succeed in *all* areas of consumption and work in which one can be deceived. In any event, it is clear that fear of fraud is one of several sources of risk of loss that has a social cost in denying people access to higher interest on their capital and to lower prices on consumer goods and services purchased on the Internet. This is the analog of other costs of social participation generated by fear of non-white-collar crimes.

In *Crime Control as Industry: Towards Gulags Western Style*, Christie (2000) elaborates the notion that particular ways of dealing with crime (and fear of crime) are important sources of profit in Western society. Students of fear of crime may find there a bridge between fear of white-collar and fear of other offenses. Businesses such as investment and long-term savings/pensions require imagery of reassurance about both competence and integrity, and much advertising takes place to sustain that branded positive *gestalt* for each firm; hence, too, the government's focus on avoiding systemic risk of general financial meltdown by rescuing or facilitating the rescue of firms such as Bear Sterns and Northern Rock. (The street crime equivalent might be sending out the National Guard or paramilitary police to stop mayhem on the streets.) Certainly one may see that both preceding frauds and in the aftermath of frauds, substantial funds are spent on fraud-risk management, with in most areas of activity, very imperfect knowledge of actual risk levels. In the case of international businesses deciding where to locate, reputation for (low) crime presumably is one of many factors comprising attractiveness, and this affects key staff judgments not

[27] The fact that fear is unproductive in practical terms does not of course mean that it is not experienced as an emotion. It is intriguing to think about what 'fight or flight' means in the context of fraud, except perhaps when Mafiosi are making offers one cannot refuse.

only as it relates to the workplace but also residence and schooling: but specific fraud risks are unlikely to feature heavily except where locally recruited staff untrustworthiness is seen to be endemic. Detailed area-based information regarding crime risks is seldom available (though corporate security staff might be asked for briefings), and there is no evidence about how often it is requested or how salient it would be if available. Some crime risks, such as fraud risks, would seldom be local in nature anyway. As for residents, their risks of being defrauded *by* businesses would be unlikely to be material in decisions where to live: as Croall (2001) notes – though one should *caveat* that her research preceded the growth of neighborhood supermarkets in the United Kingdom – most of the food and drugs violations that are prosecuted are committed by small, local shops, and if people knew they were being cheated, most could shop elsewhere unless there were large price differences. Poor people have little choice where to live anyway, and they may be regular targets for consumer fraud. If staff thought that employers were stealing their national insurance/Social Security contributions or, *a fortiori,* their occupational pension funds, this might make a considerable difference to their choice of employer: but if they had this knowledge, the frauds probably would not be allowed to be perpetrated.[28]

Cities, and fear of crime within them, remain relevant to business survival and prosperity, but to the extent that the locus of economic regeneration has shifted to dematerialized factors of production such as global financial services which have little sunk capital, business location – though still tied to cultural capital, reservoirs of expertise, prestige and plausible commutability for staff – is more flexible than it was within as well as between nations. Consequently, the commercial impact of fear of urban crime in general and fraud in particular has shifted. Where goods (rather than electronic services, which include pornographic services) have to be delivered physically, there is some nexus between fear of crime and business in the city, since that is where many consumers will remain. The depth of this effect may depend on the growth of e-business, and the propinquity of other deal makers and clients will continue to favor the continuation of the financial district as a place rather than a pure abstraction, even though deals have increasingly become transnational, as financial institutions merge to enable them to offer one-stop financial shopping to clients (and, doubtless, for other less customer-led reasons). Such mergers accelerated after the financial services crashes of 2008.

For élites, the ability to insulate themselves personally from risk of common crimes is important. However, although much has been written about the central-

[28] However, the post-Maxwell pension fund fraud reforms to company pensions in the mid-1990s did not give workers the right of representation as pension fund trustees, reflecting the UK government's fear of upsetting employers. Enron employees – unlike their directors - famously were forbidden to sell Enron shares in the run up to corporate failure. Enron instituted a "lockdown," which prevented employees from selling their shares of Enron stock between October 26, 2001 and November 13, 2001, while the company spiralled into bankruptcy. According to Enron, the lockdown was administratively necessary for the company to proceed with a desired change of the pension plan's trustee and record keeper; however it conveniently reduced the level of stock sales and thus kept the share price higher than it otherwise would have been. Enron employees, 62% of whose pension scheme – or 401(k) plan – consisted of Enron stock, lost as much as $1bn in funds.

ity of trust in late modern as well as in early modern commerce, fraud risks are usually judgments about particular individuals or about ethnicities/national origins (e.g., Nigerians, Russians) with whom one may be dealing professionally, which may be assessed by 'due diligence' conducted by professionals. (In other arenas, of course, elites may be victims of identity fraud, card counterfeiting, etcetera, but their losses from these are relatively immaterial.) Protection from terrorism, extortion, kidnapping for protest or for profit, ecoprotests, and cybercrime, as well as from the more traditional forms of crime, becomes part of the security quilt around urban financial services, and the City of London's Ring of Steel, supported by extensive police video surveillance in the streets (though not in the boardroom), becomes the equivalent of the Gated City, with crime reductive effects at least in areas where the poor and other sources of threat are not already inside. These commercial risks may vary considerably between countries: corruption, extortion, and kidnap and ransom are a far larger problem in many eastern European and Latin American countries than in most industrialized countries (Mayhew et al., 1997; van Kesteren et al., 2001; van Dijk et al., 2007), excepting parts of Italy. Elsewhere, the industrial estate, the shopping mall, and local corner shop have their own diverse problems of security, involving insecurities about transportation of customers and staff to and from the premises as well as about the security of buildings and contents from burglary, criminal damage, fraud, robbery and theft. The effects of fear on business and the collateral effects of this remain underexplored empirically and conceptually. The business context of crime and fear in urban space has been neglected in criminological literature and research, but despite the growth of e-tailing, it remains relevant, especially for areas in which access to home computers is limited not just by poverty but by the abnormally high risks of having computers stolen.

Frustrating though it may be for fraud departments of major corporations, however, their senior executives seem more fixated on their performance targets and consequent bonuses for the coming year than on strategic fraud reduction which may cost them substantial upfront expenditure which may not produce a yield within their period of company stewardship: so on a 'willingness to pay' measure of fear or concern, directors clearly are not fearful enough, most of the time. An exception is the massive multi-billion dollar investment of United Kingdom and other European card issuers in Chip and PIN to reduce losses from 'card present' frauds. Fuelled by regular media reports about e-invasions, public anxieties about 'identity theft' – and losses to banks themselves from 'card not present' (e.g., Internet) transactions – will doubtless lead to further expenditure on authentication of users, but in the United States particularly, identity duplication remains an omnipresent risk. It remains to be seen whether in the case of the variety of forms of fraud, there are sufficient 'capable guardians' (in the language of situational opportunity 'theory') with the organizational power and legitimacy both to reduce risks objectively and to reassure the public that (with apologies to Roosevelt) the only thing they have to fear is fear itself.

Acknowledgments The author is grateful for the Economic and Social Research Council Professorial Fellowship RES-051-27-0208, under whose auspices this research was conducted.

References

Babiak, P. and Hare, R. (2006) *Snakes in Suits: When Psychopaths Go to Work*, New York: Harper Collins.

Baum, K. (2006) *Identity Theft, 2004*, Washington DC: Bureau of Justice Statistics.

Baum, K. (2007) *Identity Theft 2005*, Washington DC: Bureau of Justice Statistics. http://www.ojp.usdoj.gov/bjs/pub/pdf/it05.pdf.

Black, W. (2005) *The Best Way to Rob a Bank is to Own One: How Corporate Executives and Politicians Looted the S&L Industry*, Austin TX: University of Texas Press.

Christie, N. (2000) *Crime Control as Industry: Towards Gulags Western Style*. London: Routledge.

Coates, J. and Herbert, J. (2008) Endogenous steroids and financial risk taking on a London trading floor, *PNAS April 22, 2008*. vol. 105, no. 16, 6167–6172.

Computer Security Institute (2007) *CSI Survey 2007*. http://www.gocsi.com.

Croall, H. (2001) *White-Collar Crime*. 2nd ed., Milton Keynes: Open University Press.

Demos (2006) *The Business of Resilience* http://www.demos.co.uk/publications/thebusinessofresilience.

Ditton, J., Chadee, D., Farrall, S., Gilchrist, E. and Bannister, J. (2004) From imitation to intimidation: a note on the curious and changing relationship between the media, crime and fear of crime. *British Journal of Criminology* 44(4): 595–610.

Dijk, J. van, Manchin, R., Kesteren, J. van, Nevala, S. and Hideg, G. (2007) *The Burden of Crime in the European Union*. http://www.gallup-europe.be/euics/Xz38/downloads/EUICS%20-%20The%20Burden%20of%20Crime%20in%20the%20EU.pdf.

Dorn, N. and Levi, M. (2007)European Private Security, Corporate Investigation and Military Services: Collective Security, Market Regulation and Structuring the Public Sphere, *Policing and Society*, 17(3): 213–238.

Dorn, N. and Levi, M. (forthcoming). Private-public or public-private? Strategic dialogue on serious crime and terrorism in the EU. *Security Journal*.

Financial Services Authority (2007) *Financial Outlook, 2006*, London: FSA.

Gabriel, U. and Greve, W. (2003)Fear of crime: towards a psychological approach. *British Journal of Criminology*, 43: 600–614.

Gardner, D. (2008) *Risk: the Science of Politics and Fear*, London: Virgin.

Gill, M. (ed.) (2006) *The Handbook of Security*, London: Palgrave Macmillan.

Goodey, J. (1998) Doing research on 'fear of crime, boys, race and masculinities': utilizing a feminist standpoint epistemology. *International Journal of Social Research Methodology*. 1(2): 137–152.

Goodey, J. (2005) *Victims and Victimology: Research, Policy and Practice* London: Pearson Education.

Grabosky, P. and Smith, R. (1998)*Crime in the Digital Age*, London: Transaction.

Ichheiser, G. (1944) Fear of Violence and Fear of Fraud: With Some Remarks on the Social Psychology of Antisemitism. *Sociometry* 7(4): 376–383.

Innes, M. (2004) Signal crimes and signal disorders: notes on deviance as communicative action. *The British Journal of Sociology*, 55(3): 335–355.

Jackson, J. (2004) Experience and expression: social and cultural significance in the fear of crime. *British Journal of Criminology* 44: 946–966.

James, M., Graycar, A. and Mayhew, P. (2003) *A safe and secure environment for older Australians*. Research and public policy series no. 51. Canberra: Australian Institute of Criminology http://www.aic.gov.au/publications/rpp/51.

Javelin Strategy and Research (2007) *Identity Fraud Survey Report 2007*. http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf.

Kane, J. and Wall, A. (2006) *The National Public Household Survey 2005*, Virginia: National Center for White-Collar Crime.

Jones, T. and Newburn, T. (2006a) Three Strikes and You're Out: Exploring Symbol and Substance in American and British Crime Control Politics. *British Journal of Criminology,* 46(5): 781–802.

Jones, T. and Newburn, T. (2006b) *Policy Transfer and Criminal Justice*, Milton Keynes: Open University Press.

Kesteren, J. van, Mayhew, P. and Nieuwbeerta, P. (2001) *Criminal Victimisation in Seventeen Industrialised Countries: Key Findings from the 2000 International Crime Victims Survey*. http://www.unicri.it/wwd/analysis/icvs/pdf_files/key2000i/index.htm.

Killias, M. (1990) Vulnerability: towards a better understanding of a key variable in the genesis of fear of crime. *Violence Vict.* 5(2):97–108.

LaGrange, R.L. and Ferraro K.F. (1987)The elderly's fear of crime: a critical examination of the research. *Research on Ageing* 9: 372–391.

Levi, M. (2001) 'Between the risk and the reality falls the shadow': Evidence and urban legends in computer fraud, *Crime and the Internet* D. Wall (ed.), London: Routledge. 44–58.

Levi, M. (2006) 'The Media Construction of Financial White-Collar Crimes', *British Journal of Criminology*, Special Issue on Markets, Risk and Crime, 46: 1037–1057.

Levi, M. (2008) 'White-collar, organised and cyber crimes in the media: some contrasts and similarities', *Crime, Law and Social Change*, 10.1007/s10611-008-9111-y.

Levi, M. and A. Pithouse (forthcoming) *White-Collar Crime and its Victims*, Oxford: Clarendon Press.

Levi, M., Burrows, J., Fleming, M. and Hopkins, M. with the assistance of Matthews, K. (2007a) *The Nature, Extent and Economic Impact of Fraud in the UK*. London: Association of Chief Police Officers. http://www.acpo.police.uk/asp/policies/Data/Fraud%20in%20the%20UK.pdf.

Levi, M., Maguire, M. and Brookman, F. (2007b) Violent Crime. *The Oxford Handbook of Criminology* M. Maguire, R. Morgan and R. Reiner (eds.), Fourth Edition, Oxford: Oxford University Press.

Mann, D. and Sutton, M. (1998)'NetCrime: more change in the organisation of thieving', *British Journal of Criminology*, 38, 201–229.

Mayhew, P. and van Dijk, J. (1997) *Criminal Victimization in Eleven Industrialised Countries*, The Hague: WODC, Ministry of Justice.

Pew (2006) *Are "Wired Seniors" Sitting Ducks?* http://www.pewinternet.org/pdfs/PIP_Wired_Senior_2006_Memo.pdf.

Pew (2007) *Spam 2007 Data Memo*, http://www.pewinternet.org/pdfs/PIP_Spam_May_2007.pdf.

Rountree, P. (1998) A Reexamination of the Crime-Fear Linkage. *Journal of Research in Crime and Delinquency*, 35(3): 341–372.

Semmens, N. (2003) *Fear of Plastic Fraud.* unpublished Ph.D. thesis, University of Sheffield, UK.

Skogan, W. (1995) Crime and the Racial Fears of White Americans. *The Annals of the American Academy of Political and Social Science*. 539(1): 59–71.

Titus, R. and Gover, A. (2001)Personal Fraud: The Victims and the Scams. *Repeat Victimization* G. Farrell and K. Pease (eds.), Monsey, NJ: Criminal Justice Press.

Wall, D. (2008) "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime". *International Review of Law, Computers and Technology*, 22(1–2): 45–63.

Warr, M. (2001) Fear of crime in the United States: Avenues for Research and Policy. *Criminal Justice 2000*, Vol.4 Measurement and Analysis of Crime and Justice: 451–489. http://www.ncjrs.gov/criminal_justice2000/vol_4/04i.pdf.

Whimster, S. (ed.) (1992) *Global Finance and Urban Living: A study of Metropolitan change,* London: Routledge.

Wilson, S. (2006) Law, morality, and regulation: Victorian experiences of financial crime. *British Journal of Criminology,* 46: 1073–1090.

Wilson, D., Patterson, D., Powell, G. and Hembury, R. (2006) *Fraud and technology crimes: Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources*, http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf.