Foreword: some reflections on the evolution of economic and financial crimes

Michael Levi[1]

DEFINITIONS AND A TYPOLOGY OF FINANCIAL CRIME HARMS

'Financial crime' is normally not a legal but rather an administratively functional category and has been growing in use, especially in OECD countries, though in continental Europe and parts of Africa, 'economic crime' is more commonly used and overlaps extensively.[2] A lightly grounded paper by the IMF (2001: 3) defines it very broadly beyond economic crime or crimes in the financial sector, prefiguring the extension of money laundering offences to the proceeds of all crimes for financial gain:

> Financial crime, which is a subset of financial abuse, can refer to any non-violent crime that generally results in a financial loss, including financial fraud. It also includes a range of illegal activities such as money laundering and tax evasion. Money laundering refers to activities involving the processing of criminal proceeds to disguise their association with criminal activities.

At the 11th UN Crime Congress, the UNODC (2005: 1) adopted a fairly protean view:

> '[E]conomic and financial crime' refers broadly to any non-violent crime that results in a financial loss. These crimes thus comprise a broad range of illegal activities, including fraud, tax evasion and money-laundering. The category of 'economic crime' is hard to define and its

[1] Michael Levi, PhD, DSc (Econ.), Professor of Criminology, Cardiff University. Levi@Cardiff.ac.uk.

[2] The major developing country with a reputation for fraud, Nigeria, calls its central agency, established in 2004, the Economic and Financial Crimes Commission, though the difference between 'economic' and 'financial' is not elaborated. To some extent this is semantic pedantry, as issues of jurisdiction are often set out in legislation. It may be that 'economic' is seen as wider than 'financial', since it might cover agricultural, industrial and service sector corruption, scams and environmental crimes that go beyond the financial services frauds (contrary to s.419 of the Nigerian Criminal Code) for which Nigerians have long enjoyed an unenviable reputation worldwide. The UK Treasury and Financial Services Authority had 'financial crime' sections, reflecting their remit for financial services. (Though in mid-2015, the Treasury refined this into Financial Sanctions and Anti-Money Laundering and Terrorism Finance, and the Financial Conduct Authority has simply 'Enforcement and market oversight' and 'Risk and compliance oversight' divisions, so 'financial crime' has vanished from history.) The City of London police – the 'lead force' for fraud investigations in England and Wales – calls its unit the 'Economic Crime Department' and the National Crime Agency – created in 2012 – places its fraud work within the 'Economic Crime Command'.

> exact conceptualization remains a challenge. The task has been further complicated by rapid advances in technology, which provide new opportunities for such crimes.

In addition to its central role in the UN Convention against Corruption and further anti-corruption efforts, the main component in the UN's construct of economic crime appears to be fraud and identity-related crime (UNODC, 2011).

The growth of financial crime as a term reflects the extension of the crime control functions of states internationally under the pressures of 'mutual evaluation', a key part of which is the consequent superintending (or 'responsibilisation') of the private sector against 'crimes of globalisation' (Favarel-Garrigues et al., 2011; Levi and Gilmore, 2002; Levi, 2010). Collectively, other terms used to package these diverse activities include 'threat finance' (Levi, 2010) or 'illicit finance', chosen by HM Treasury in the UK, and 'Terrorism and Illicit Finance', for the US Treasury.

Prior to the 21st century, to the extent that the term was used at all, 'financial crime' meant just fraud and, later (from the late 1980s), money laundering. Indeed, the administrative agency created in 1990 as part of the US Treasury to process reports from banks on large currency deposits, cross-border cash and wire transfers, and others required under the Bank Secrecy Act 1970 and money laundering legislation, was called the Financial Crimes Enforcement Network (FinCEN). However, its scope and that of the criminal law and financial services/corporate regulation have been expanding at frequent intervals since the 1990s. 'Financial crime' now includes:

1. frauds of different types with different victims (from wealthy corporates and High Net Worth Individuals to the very poor and from very rich to very poor governments);
2. 'market abuse' such as insider dealing/trading (which covers a range from corrupt relationships between investors and insiders to giving talks about company prospects to some important analysts before releasing results to the general market);
3. money laundering (of all crimes, increasingly including tax fraud[3]);
4. financing of terrorism (mostly since 2001) and (since 2008) of Proliferation Financing, including Weapons of Mass Destruction (WMD); and
5. transnational bribery (usually by corporates paying public officials in developing countries, but also in their own – wealthy or poor – countries).

Some of these offences – like fraud – are longstanding, though even there, legislative changes have been needed (as is the case with the Fraud Act 2006 in the UK, excepting Scotland where common law currently is retained), for example to cope with

[3] Though countries vary substantially in how they define 'tax fraud'. Switzerland for example restricts it to active deception (e.g. falsification of data in tax submissions made to it), excluding omissions and non-reporting of tax obligations elsewhere. So if someone with a Swiss account does not need to file tax documents in Switzerland, they cannot commit tax fraud there and cannot normally be extradited for this. On the other hand, since 2008, there has been a great deal of international action on mutual cooperation in tax matters and in withholding tax arrangements, though these too are subject to sophisticated avoidance mechanisms. See de Willebois et al. (2011), Sharman (2011) and Shaxson (2011) for good contemporary analyses.

computer-enabled crimes. Others are new since the 1980s (such as insider dealing/trading and money laundering); while others still typically are only a few years old or are in a process of major adaptation (like financing of terrorism and nuclear proliferation, and transnational bribery). In addition, offences involving Intellectual Property can be treated as part of 'financial crime', if only via their role (with all other offences) as part of the ever-extending list of 'predicate crimes' for money laundering offences. Indeed, to the extent that most crimes for gain lead to concealment or transformation of *some* proceeds, it is arguable that all such crimes *ipso facto* become 'financial crimes' and thereby those who facilitate them and the movement of moneys from them are liable to increased risks of 'criminalisation', at least in principle. It may be useful to regard 'financial crime' and its sub-sets – 'money laundering' and 'corruption' – as floating signifiers, a moral category of illicit capitalism which contains whatever pressure group politics succeeds in placing therein. An almost universal core component of this is the passage of criminal laws and regulatory processes meeting evolving Financial Action Task Force (FATF) criteria. For example, anti-money laundering legislation (AML) must now cover both tax evasion and the financing of WMD proliferation (FATF, 2012).

Although the pressure to show evidence of harm reduction from control measures is an especially British development, paralleled in Australia, the Netherlands, Sweden and some other parts of the EU (and the European Commission itself), 'crime control' is often a matter of expressing values rather than science (or pseudo-science) in many parts of the globe. Even in those countries where evidence-based policing is not a mantra, however, *some* performance data are called for, though countries struggle to utilise sensibly their analytical value as proxies for effectiveness. The FATF and FATF-style evaluations ask countries to show evidence of performance in AML by the number of criminal laundering prosecutions. The easiest way to please the evaluators is to prosecute more self-laundering cases and thus increase *recorded* 'money laundering' and 'financial crimes'. Halliday et al. (2014) were rather critical of the Third Round FATF evaluation process, likening it at times to the Tsarist Potemkin Villages in which an appearance of compliance and formal structures were often sufficient to impress and to get a good compliance score. It remains an open question to what extent this will change in the more reality and outcome-focused Fourth Round using the significantly revised FATF (2013) Methodology. What is clear is that the majority of countries have begun already to experiment with National Risk Assessments based around this evaluation process.

There have been few attempts to develop a coherent policy for all the disparate acts that fall under the umbrella term 'financial crime', nor is there any obvious prioritisation outside acts regarded as important for 'national security' and the interests of corporate capital, such as protection from (primarily Iranian) financing of nuclear proliferation and from broader state-sponsored attacks on corporate/national infrastructure cybersecurity. The control of at least some of the offences in the five sub-categories above has become the responsibility of national regulators of financial services and (at least in Europe, where regulation is broader) of the professions, often termed 'gatekeepers' (Gilmore, 2011). Curiously, this regulatory remit excludes most frauds by volume, since in the UK, for example, only those committed against *or by* regulated firms that achieve the undefined category of 'significant' are in scope, and

even there, nothing is known about the follow up to such reports. The criminalisation of transnational (and sometimes national) bribery affects banks directly via risks (should they fail to report any suspicions they may have) of money laundering charges (1) against their own individual Money Laundering Reporting Officers (who are required by regulators to be appointed and approved by them as part of the 'responsibilisation process') and (2) perhaps against the banks themselves. It also affects banks indirectly because of the risks (however remote in practice) that companies to whom they have lent money might be damaged by severe penalties should *they* be convicted of corruption. The implications of these developments are important. When senior staff on the best-selling UK tabloid newspapers *The Sun* and the (now closed) *News of the World* were arrested and accused of bribing the police and other public officials, this created global risk for the Murdoch *News International* corporation in the US under the extra-territorial provisions of the Foreign Corrupt Practices Act 1977 (FCPA) in ways that were doubtless not envisaged by the media staff if and when they 'bought' the information for the stories.

As used in different countries, 'financial crime' and 'economic crime' comprise crimes with different categories and levels of harm, committed by and impacting upon highly diverse sectors of the population. Their sub-components are investigated (and investigat*able*) by very different policing and regulatory methodologies both before and after 'crime' commission. Because of this, it is difficult to see what purposes the terms serve except to differentiate them from street and household crime and, unintentionally perhaps, to obfuscate which resources are being given to or withheld from investigating particular sorts of activities. Close analysis by Gannon and Doig (2010) detailed the unannounced drift of investigative attention in England and Wales from serious fraud to the financial assets of general criminals within the overall rubric of 'financial investigation' (though this was partly counter-balanced by the employment in the UK of civilians, often ex-police, as financial investigators). This is paralleled with the drift in resource in banks from fraud structures within compliance to financial crime departments that also may deal with money laundering and sanctions. Money laundering offences can arise in principle from drugs trafficking or from any crime for gain, including all forms of fraud; terrorist financing and the financing of proliferation can come from both licit and illicit sources, and primarily probably come from licit sources (including, but by no means restricted to, countries like Iran that are defined as 'rogue states'). As a legal category, 'laundering' does not enable us to distinguish between professional money launderers, people who launder money from their own crimes (like burglars putting money into their own bank accounts in their own names), and banks who intentionally or recklessly ignore their obligations to report suspected money laundering or who turn a wilfully blind eye to 'smurfing' by customers to fall below the $10,000 reporting threshold in the US and the €15,000 threshold in the EU, which will fall to €10,000 under the Fourth Money Laundering Directive.[4]

[4] To give some idea of the scale and potential consequences, in 2010, Wachovia Corp. – which by then had merged with Wells Fargo Bank in the aftermath of the financial crisis – agreed in a deferred prosecution agreement to pay $160 million in forfeitures and fines for allowing the laundering of at least $110 million in drug proceeds. US federal prosecutors had accused it of 'willfully' overlooking the suspicious character of more than $420 *billion* in

A particular practical complication is that although we normally conceive of victim–offender or consensual crime relationships – whether violent or for financial gain – as occurring *within* countries, many significant financial crimes (not *just* cybercrimes) occur between people in *different* legal jurisdictions, at least at some stages in the criminal supply chain, from production/planning to money laundering. We therefore need a greater breakdown of sub-types to make sense of these acts, which also are problematic to capture in national crime and justice statistics, that are important signals to society of the moral state of the nation and need to be modernised to take account of these developments in the forms of crime. Let us briefly set out the interests affected by different sorts of financial crime in the context of reactions to them.

CRIMINALISATION AND DOMESTIC AND INTERNATIONAL POLITICAL PRESSURES

The link between globalisation and crime often lacks clarity (Karstedt, 2012), nor is internationalisation of trade or crime as new as is sometimes claimed. However, one of its consequences is to call into question the autonomy of national law-making. Crimes of any kind are the product of a political process, but the politics of crime creation and enforcement in the 'new crimes of globalisation' raise particularly interesting issues. Other countries apply pressure – as they have always done militarily and politically – to accommodate to their interests and their legal protections. After the Robber Baron era of the 19th century in the US, there have been sustained pressures to criminalise transnational bribery and cartels in the interest of market cleanliness and fair competition. Yet different legal traditions, cultural/ideological forces and constellations of interests play themselves out in different ways. The US criminalised cartels in the Sherman Act 1890; it took over a century for the UK government to be persuaded that

---

transactions between the bank and Mexican currency-exchange houses. Details of the agreement are given at http://www.justice.gov/usao/fls/PressReleases/100317-02.html. The rhetoric of the press release of this agreement is interesting. US Attorney Jeffrey H. Sloman stated, 'On the heels of the UBS international banking case, in which we held accountable the largest bank in Switzerland, today we announce the deferred prosecution of Wachovia, one of the largest banks in the United States. Wachovia's blatant disregard for our banking laws gave international cocaine cartels a virtual carte blanche to finance their operations by laundering at least $110 million in drug proceeds. Corporate citizens, no matter how big or powerful, must be held accountable for their actions. Today's historic agreement makes it clear that such conduct will not be tolerated and imposes the largest penalty in any BSA case prosecuted to date.' For media reports see, inter alia, http://www.guardian.co.uk/world/2011/apr/03/us-bank-mexico-drug-gangs?CMP=twt_fd and http://articles.latimes.com/2011/nov/27/world/la-fg-mexico-money-laundering-banks-20111128. In December 2011, Wachovia settled a further deferred prosecution agreement with the anti-trust division of the Department of Justice in relation to bid-rigging scams. 'Fortunately', the 12 month probationary period of the failure to institute proper AML procedures agreement had lapsed by then, or the (ex) bank would have had to be prosecuted, with consequences that it might have to be closed, certainly after conviction. A set of other banks – including, most famously, HSBC – were later the subject of monitorships, settlements and Deferred Prosecution Agreements.

this offence against capitalist level playing field principles merited criminalisation, in the Enterprise Act 2002, something that is still not an accepted approach in continental Europe.[5]

Money laundering and insider trading were not criminal offences in Europe before the late 20th century: again the US led the way, with the UK following, and other countries came in their wake. The counterfeiting of Intellectual Property has become a much more significant economic issue since the 1980s, with the rise of global brands and the development of digital copying and mass production techniques, though some countries have long prohibited false labelling in addition to currency counterfeiting. However, the global criminalisation of such 'piracy' has been a more tentative and controversial area, touching upon everyday activities such as file sharing that are not seen as 'truly criminal', especially not by younger people.

In countries such as the UK (and indeed the EU as a whole), Regulatory Impact Assessments have to be made when legislation is presented, and the public has to be 'prepared' by lobbying campaigns involving estimates of harm as well as appeals to values. An important role is played in this struggle by data – however poorly evidence based – about harmfulness of the activity, which gains media purchase and usually gives an advantage to advocates of change. Thus, advocates of tough responses to Intellectual Property violations seek to rebrand those activities as 'copyright theft' and (like credit card issuers) to increase their perceived harm by associating them with 'organised crime' and 'terrorist finance'. The music and film industries – as well as heavy R & D sectors such as pharmaceuticals – have lobbied hard for the reprioritisation of such acts as 'real crimes', and both President Obama and UK ministers have stressed the centrality of protecting Intellectual Property to the economic prosperity of their countries.[6] An industry and government-financed police unit has been set up within the City of London police economic crime department. Similarly, with regard to cybercrimes, a report by technology firm Detica, badged alongside the Office of Cyber Security in the Cabinet Office, typically noted that its (in fact imaginatively high guesstimated) data were at the low end of the probable range (Detica and Office of Cyber Security and Information Assurance 2011):

> In our most-likely scenario, we estimate the cost of cyber crime to the UK to be £27bn per annum. … In all probability, and in line with our worst-case scenarios, the real impact of cyber crime is likely to be much greater. Although our study shows that cyber crime has a considerable impact on citizens and the Government, the main loser – at a total estimated cost of £21bn – is UK business, which suffers from high levels of intellectual property theft and espionage. Businesses bearing the brunt of cyber crime are providers of software and computer services, financial services, the pharmaceutical and biotech industry, and electronic and electrical equipment suppliers.

---

[5] This criminalisation was encouraged by the US authorities, keen to find a route for extradition to the US of UK residents involved in price-fixing and other business violations.

[6] Though the Congressional debates in early 2012 over failed proposals in the Stop Online Piracy Act and the PROTECT IP Act to penalise websites and Internet Service Providers that allow Intellectual Property protected material to be downloaded revealed that the financial and cultural power of the 'new networked media', combined with consumer hostility to high-priced music and movies, could triumph over the traditional Hollywood and media pressure groups.

The cybercrime cost data did not impress the specialist computer press, but became 'facts-by-repetition' via their reuse in political speeches. A later study co-authored by this writer heavily critiqued this effort (Anderson et al., 2012), but subsequent cyber-attacks and revelations about their sources in China and Russia (as well as in Western countries) have illustrated that the scale of *risk* is very high, whatever the disputed figures in any one year.

The heightened political profile of fraud, scandal and allegations of conflicts of interest played a much more prominent role in influencing legislation since the 1980s than earlier in the 20th century in the UK, though not necessarily in the US, given New Deal responses to the Wall Street Crash of 1929 and the subsequent economic crisis.

CONCLUSIONS

In a profound early study, Aubert (1952: 263) argued that the ambiguity of white-collar crime and its control was a stimulant to be analysed rather than to be definitionally resolved by fiat. He added:

> One main obstacle to the development of a fruitful theoretical orientation is to be found in the tendency to treat criminal behavior, on the one hand, and the system of legal sanctions, on the other, as two separate problems. In our opinion, crime and punishment are most fruitfully handled as two aspects of a group process or two links in a specific type of social interaction.

Despite their growing use as terms, it is not sensible to take 'financial crimes' or 'economic crimes' as a singular category for analytical or policy purposes, and we might be better served by breaking them up into clearer areas of criminal activity. So what purposes does the phrase serve? 'Financial crime' is largely a term of political and bureaucratic convenience. The analysis above illustrates that there are a multitude of political and economic pressures that lead to the criminalisation of various forms of what might be termed white-collar and organised crimes that fall under this single label. These pressures are often reactions to national scandals or international events (like the Global Financial Crisis), or to national/international mobilisations of non-governmental organisations and intergovernmental bodies, including constitutionally informal ones like the FATF. The economic imperatives of competition between nations for business and professional elites to locate there may have to be balanced against efforts by political elites to shore up their legitimacy, for example after corruption or egregious tax scandals such as those involving Luxembourg in 2014. These pressures mean that the responses to various 'financial crimes' differ between jurisdictions.

To conclude, both in the forms of financial crime often labelled separately as 'organised crime' and 'white-collar crime', there are many overlaps and convergences which are reflected in their policing, sometimes by accident and sometimes by design. But it is important to look analytically at what *forms* of serious crime for gain are being targeted, by whom and using what methodologies. So far, the convergence in methods of policing fraud and policing organised crime targets principally the drift by 'the usual suspects' into fraud and Intellectual Property crimes and their tracking by police using financial investigations, data from AML Suspicious Activity Reports and other recent techniques of data warehousing and network analysis. These changes do not represent a

radical shift towards reprioritising elite frauds and Grand Corruption over 'the usual crimes', but they do represent varying attempts by modern governments and policing/regulatory institutions to manage emerging public threats to individuals, business and government without imperilling conventional law and order issues.

Professor Barry Rider, personally, and the annual gatherings at the Economic Crime Symposium, some fruits of which are represented in this handbook, have played an important role in identifying and managing these profound social risks. It is a depressing fact that the conclusions of my study of problems in fraud trials for the Commonwealth Law Ministers Conference in 1982, arising from discussions with Professor Rider at the earliest Economic Crime Symposia, might still be applied today, though with additional complications from electronic and mobile phone evidence that (like those products themselves) did not exist in 1982. One of the effects of the AML and anti-corruption movement has been to generate far more similarity in national legislation and mutual legal assistance than would have occurred otherwise, but the impact of this on international asset freezing and recovery remains a work in (slow) progress. *Quo vadis*? Predicting the past is far easier than predicting the future! But this volume reflects the worthy efforts of some in the international community to grapple with Global Bads, which it would be more realistic to see as aiming to reduce harm than to eliminate it altogether. But first, we need to work harder on how we can judge whether things are truly improving or getting worse, and that requires both collective action and collective thought. This handbook represents a stage along that long road.

REFERENCES

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. Levi, M., Moore, T. and Savage, S. (2012) 'Measuring the cost of cybercrime', http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

Aubert, V. (1952) 'White-collar crime and social structure', *American Journal of Sociology*, 58 (3): 263–271.

Detica and Office of Cyber Security and Information Assurance (2011) *The Cost of Cyber Crime: A Detica and Cabinet Office Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*, http://www.baesystemsDetica and Cabinet Office.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf.

FATF (2012) *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*, Paris: Financial Action Task Force.

FATF (2013) *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CTF Systems*, Paris: Financial Action Task Force.

Favarel-Garrigues, G., Godefroy, T. and Lascoumes, P. (2011) 'Reluctant partners? Banks in the fight against money laundering and terrorism financing in France', *Security Dialogue*, 42 (2): 179–196.

Gannon, R. and Doig, A. (2010) 'Ducking the answer? Fraud strategies and police resources', *Policing and Society*, 20 (1): 39–60.

Gilmore, B. (2011) *Dirty Money*, Strasbourg: Council of Europe Press.

Halliday, T., Levi, M. and Reuter, P. (2014) *Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism*, Chicago: American Bar Foundation, http://www.lexglobal.org/files/Report_Global%20Surveillance%20of%20Dirty%20Money%201.30.2014.pdf.

IMF (2001) *Financial System Abuse, Financial Crime and Money Laundering – Background Paper*, Washington DC: International Monetary Fund.

Karstedt, S. (2012) 'Globalization and crime', in G. Ritzer (ed.), *Wiley-Blackwell Encyclopedia of Globalization*, Oxford: Wiley-Blackwell.

Levi, M. (2010) 'Combating the financing of terrorism: A history and assessment of the control of "threat finance"', *British Journal of Criminology Special Issue Terrorism: Criminological Perspectives*, 50 (4): 650–669.

Levi, M. and Gilmore, W. (2002) 'Terrorist finance, money laundering and the rise and rise of mutual evaluation: A new paradigm for crime control?' *European Journal of Law Reform*, 4 (2): 337–364.

Sharman, J. (2011) *The Money Laundry: Regulating Criminal Finance in the Global Economy*, Ithaca: Cornell University Press.

Shaxson, N. (2011) *Treasure Islands: Tax Havens and the Men Who Stole the World*, London: Bodley Head.

UNODC (2005) *Economic and Financial Crimes: Challenges to Sustainable Development*, Vienna: United Nations Office on Drugs and Crime.

UNODC (2011) *Thematic Programme on Action against Corruption and Economic Crime (2010–2011)*, Vienna: United Nations Office on Drugs and Crime.

de Willebois, E., Halter, E., Harrison, R., Park, J. and Sharman, J. (2011) *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, Washington DC: The International Bank for Reconstruction and Development/The World Bank.