Topicality of research

September 2009

Penal Issues

CESDIP
Centre de Recherches Sociologiques sur le Droit et les Institutions Pénales
UMR 8183

www.cesdip.fr

Combating Money Laundering : Sentinels and Tools at Work

Gilles FAVAREL-GARRIGUES *(CERI-Sciences-Po),* ***Thierry GODEFROY*** *(CESDIP) and* ***Pierre LASCOUMES*** *(CEVIPOF-Sciences-Po)* *report on a survey of anti-money laundering professionals. This issue of Penal Issues focuses mostly on the implementation of surveillance and reporting schemes by banking organisations.*

Twenty years ago, in July 1989, the Paris conference of the G7 launched the international fight against the laundering of money derived from drug trafficking and set banks in the forefront of this combat by entrusting them with the surveillance of financial flows. This surprising innovation, contradicting the most firmly anchored principles of the profession (non-intrusion in the economic decisions of clients and strict confidentiality with respect to outside actors, barring some strictly limited administrative and judicial exceptions) has met with enormous international success. The message was given wide circulation and the fight was institutionalised. Gradually, all countries adopted the international anti-money laundering norms and the new international agency, the Financial Action Task Force created at the end of the Arch Summit has been assigned new missions, extending to new targets (the funding of terrorism, nuclear proliferation).

Methodology

This research is based on over seventy interviews, conducted in France in two sweeps between 2005 and 2008. Some interviewees were surveyed twice, at the beginning and end of the project. Furthermore, about ten interviews were conducted with anti-money laundering officials in Switzerland. These were useful in validating our hypotheses in a different national context. Three-fourths of the interviewees were in charge of fighting money laundering within banking establishments. These professionals acted as *chief compliance officers*, coordinating anti-money laundering policies in one capacity or another within the banking establishment.

We made sure to vary the profiles of these establishments on the basis of their type of activity (retail banking, investment banking), sphere of action (ranging from global to national) and clientele (ordinary people for the « broad-based bank » or the elite for those managing large fortunes).

The survey was completed by interviews with other anti-money-laundering actors, whether those participating in the setting of legal norms at the national level (ministries of Justice and the Economy) or the international level (FATF and IMF) or those in the professional environment of the compliance officers, ranging from public regulators (the Financial Intelligence Unit TRACFIN or the Banking Commission) to private consultants and creators of specialised computer technology.

Interviews were semi-structured, using a grid including personal questions on the interviewee's career, the attractiveness of fighting money laundering, difficulties encountered, and projects, along with broader questions calling on the person's special expertise (on current affairs, practices, administration policies, the experts' milieu itself...).

In France, anti-money laundering (AML) policies have been conducted on two registers: first, criminal legislation defined a new offence (inserted in the French Public Health Code in 1987 as part of the anti-drug legislation); second, a series of obligations for professionals to conduct surveillance was created in July 1990 and later inserted in the Monetary and Financial Code). While the criminal provisions are quite severe, in practice they are totally subordinated to the surveillance system, which is much more flexible since it is in the hands of private professional actors, the first and foremost of which are banks. Banks, which were so far exclusively commercially oriented, have been required to adjust their activity to new policing missions: they must detect and when necessary report suspicious transactions. Whereas only money derived from drug trafficking was targeted at the start, the banks' scope of surveillance has gradually been expanded to financial products generated by practically all offences (all those punishable by at least one year of imprisonment) and the variety and number of professional actors involved have been extended to include not only all financial intermediaries, but also lawyers, accountants, real estate agents, directors of casinos, art dealers, people working in gambling and lotteries, and all tradespeople who receive cash payments exceeding 15,000 euros.

UNIVERSITÉ DE VERSAILLES SAINT-QUENTIN-EN-YVELINES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA JUSTICE

This surveillance and reporting scheme requires banks to monitor their clients and their transactions, and to report any suspicion to TRACFIN (an agency created for that purpose at the ministry of Finance) This financial intelligence unit receives some 12,000 reports on atypical financial operations (suspicious activity reports) yearly. Following analysis, these reports may lead TRACFIN to inform the Public Prosecutor (about 400 cases a year), who decides whether to prosecute. In 2008 the number of reports received by TRACFIN increased to over 14,000, whereas the number of those referred to the criminal justice system for potential prosecution declined lightly (see graph below).

Thus, banking institutions have gradually developed an internal structure for monitoring the risk of non-compliance and specific procedures for meeting these obligations, which are controlled by the Banking Commission. While the banks' surveillance schemes, with their screening, profiling and risk-management instruments, now cover all clients and all operations, getting the profession to cooperate was no easy matter.

Bank Reluctance to Cooperate

During the 1990s, the banks' awareness of these new requirements built up only gradually. At the end of that decade, these control provisions were very unevenly and generally only marginally operational, as a Banking Commission survey states in a never-published report whose comments were judged « disappointing and depreciative for the banking sector » by the head of the Commission at the time. Similarly, the trial known as « *Sentier II* » in which the *Société Générale* bank was accused of money laundering between 1998 and 2001 revealed that the bank's internal anti-money laundering unit was unequipped to meet those obligations. It was composed of only two people…

Things began to change in 2000-2001: the totality of establishments set up in-house schemes including specialised units, written procedures, and a staff training policy, whereas a new ad hoc specialty, the job of compliance officer, was invented. At present, the major financial networks may have somewhere between 500 to 1,000 people working on combating money laundering. Often, actually, they may exceed 2,000 if people working on related jobs such as internal audit and risk-management are included. Last, banks finally equipped themselves with expensive software, and the use of these to sift through operations and analyse customers' behaviour has become usual practice.

In exchange for their pivotal role in fighting money laundering banks won great latitude in assessing the seriousness of atypical situations. They may now adjust their surveillance – tighten or lighten it – depending on the risk, but cannot escape the requirement to file a report when they suspect an operation of covering money laundering.

This appears as a complete change, a sudden turn around caused by the combined effect of a decisive event (the 9/11 attacks and the orientation toward fighting the financing of terrorism), the indictment of several heads of large banking establishments (*Société Générale*) and insurance companies (*AXA*), and a change in types of action (henceforth based on risk evaluation).

Developing the Tools

Tools were first developed in the mid-90s on an experimental basis, and began to spread in 2001. These tools, whose conception called upon a variety of data mining techniques (computer-assisted medical diagnosis collating previous conditions; link analysis, derived from developments in criminal analysis as applied to serial killings; text analysis), converged to produce solutions for the implementation of AML.

The possibility of using automated detection systems for financial matters was first envisioned as an auxiliary to public regulation. By the mid-90s the Financial Crimes Enforcement Network (FinCEN) the agency in charge of receiving compulsory reports by banks in the United States, had to deal with over 10 million such Currency Transaction Reports. In 1994 the US Office of Technology Assessment wrote a report that finally led to the use of data mining. At the time attention also began to focus on the development of electronic money transfer systems in connection with the measures adopted in the fight against drug trafficking and terrorism. New tools offered the possibility of detecting suspicious transactions as defined by predefined external standards: lists of individuals or criteria (checks for over 30,000 euros for instance). These are prescriptive tools that dictate a decision.

Starting in 2000-2001, the new worldwide imperative of fighting terrorism financing and the new AML orientation modulating surveillance requirements according to the risk accelerated the diffusion of software tools. Lists produced by international agencies were completed by lists of at-risk individuals developed by private companies, the so-called « politically exposed persons (PEP) ». One of the leaders in this kind of information on clients (Factiva), belonging to the Dow Jones group, analyzes over 10,000 sources (newspapers, news agency stories, on-line information, corporation reports, and so on) from one hundred-odd countries, generating detailed profiles of over 500,000 individuals including 30,000 in France. The program, updated daily, can be parameterised to fit the specific risk needs targeted by the organisation. This is a semi-prescriptive tool.

The second broad category of tools is more complex. It applies risk-modelling to the analysis of customer and account behaviour. The aim is to ground decisions by discriminating between « normal » and « abnormal » practices for each client and by evidencing unapparent relations between transactions, in particular. This type of tool attempts to consider each client's specific features; to detect common money laundering patterns as well as more unusual or hitherto unknown forms; to help analyse the context (history of the client and the account, comparison with profiles of peers); last, to centralise alerts within a given organisation irrespective of the location of the operation. Very clearly, the idea is to provide compliance officers, who are sentinels, with both decision-making aids and evidence that the required control procedures have been completed. The latest tools offer a four-stage intervention: alert, investigation-analysis, follow-up of the suspicious case and automated reporting (suspicious activity reports).

Current tools tend to integrate various approaches into a single package, providing an expert system based on established facts and acknowledged norms (a list, a quantitative threshold…); a profile identification system, based on the memory of previously identified situations and linking them together to determine indicators; last, a system of continuous client evaluation, analysing all transactions and grading them for risk (low, normal, high). By generating a log of alerts, the tool provides evidence of the action undertaken, an « auditable » proof to regulators that procedures have been completed.

Tools and Sentinels in Action

Both the definition of the parameters on which they work and the interpretation of findings depend on banks, for a large part. Setting the parameters of operations is of the utmost importance, as is stressed unanimously. As one anti-money laundering official for an international bank says, « The definition of the profile depends on us, it's not given beforehand ». The resulting options are therefore a major stake, to which all actors respond on the basis of their own experience. Their point is to empirically balance two risks: on the one hand, accepting a problematic client or operation susceptible of tarnishing the establishment's reputation; on the other hand, being flooded with an unmanageable number of alerts. There are no overall

professional rules in this respect. Practice is the main stabilising factor in these choices.

Advertising for these instruments consistently emphasises their ability to facilitate compliance with national and international regulations by eliminating illegal transactions and detecting clients representing a high financial risk. But contrary to their claims, these tools are far from solving all of the problems facing account managers and compliance officers. Based on highly sophisticated technology, they generate numerous practical problems in everyday use.

There is a serious gap, as users are well aware, between the alerts generated by the tool and the actual situation they must concretely manage. For example, in the Greater Paris region establishment of one large national banking network, 45,000 alerts are generated annually. About one thousand of these « suspicious cases » will be taken seriously and will ultimately lead to the filing of one hundred-odd suspicious activity reports to TRACFIN. These figures indicate the importance of the intervention of human sentinels in reporting, notwithstanding the touted automaticity.

Lists, for one thing, have become so long that they often contain homonyms (producing « false positives »). The management of PEP lists has multiplied problems for users: « You can't keep up. There are the official lists: OFAC (5,000 to 6,000 names), EU (1,500 names[1]), France (200), and the commercial lists: PEP lists can include 275,000 names, and Factiva even has 470,000! There aren't any official lists for PEP. Providers put whoever they like on them », complains one consultant in charge of introducing these tools.

Behaviour-based profiling software is sometimes so responsive to atypical situations that it can detect any operation however slightly out of the routine (such as an unusual sum or recipient) by a regular client. In all such cases, account managers receive a message requesting information on the dossier, often after the establishment's central AML department has sifted through the alerts. It is up to these managers to do the checking. In practice, this is often limited to a phone call with the client, in spite of all the difficulties (and the risk of losing trade) involved in exchanges of this kind where a service supplier expresses suspicion. The latter still has only a limited ability to make concrete verifications. How can a client's identity be checked? When a client claims a payment was to a supplier or for an investment, how can the legal character of the transaction be ascertained? Except when opening a new account, it would take a particularly alarming situation for a bank to request to see identity documents or the original contract or invoice justifying the payment.

Conversely, while « false positives » are definitely a problem, professionals often point out another equally acute problem: that of detecting questionable operations, well disguised as ordinary trade. Illegal financial transactions in general and money laundering in particular are naturally characterised by a will to dissimulate: organising opacity is crucial, and often achieves tremendous sophistication. Resources for doing so have been multiplied by the internationalisation of exchanges and by the opportunities offered by both offshore financial centres and those establishments who, in practice, are not in step with AML policies. Last, launderers are the best specialists in surveillance techniques and are constantly adjusting their methods to the new monitoring systems in use. Operators are therefore particularly dubious of the ability of these tools to detect sophisticated frauds. As one AML officer for an international bank points out, « computerised systems are reassuring, but they don't provide much information on where the funds are sheltered. If we're talking about something off the records and it has being done in a facility in Jersey (…) I haven't seen many computer programs capable of detecting that. Often there isn't anything that draws attention to it ».

Whereas simplistic money laundering operations such as depositing or withdrawing large amounts of cash, the opening of an account by a developing country PEP, the sudden provisioning of a dormant account by a huge transfer from an unknown establishment or one on a suspect list, and so forth, are almost always detected by professionals (with the help of their tools), this is far from true for sophisticated operations, especially those channelled through « respectable » middlemen.

Does this differential management of suspicion of money laundering based on the supposed nature of the underlying offences lead, indirectly, to target some specific forms of crime? This is suggested by several of the people who were interviewed, who felt that the fight against money laundering only succeeds in stopping « petty offenders » who are unable to outsmart the detection schemes. Compliance officers, anxious to prove their efficiency, are tempted to select the most exposed targets: « We are subject to a best efforts obligation: we have to be lily white in the eyes of the Banking Commission. No-one gives a damn about the contents. So what we do is, we find petty dealers who we have no interest in having as clients anyway. That way we identify them and eliminate them from our clientele ».

Vague Profiling and Breaches of Civil Rights

Reservations have also been expressed about the profiling techniques on which these tools rest to a large extent. The questionable points uncovered in our survey, conducted in France and Switzerland, are much the same as those advanced in US and British studies[2]. Controversies revolve around three focuses: principled issues on profiling, practical problems of implementation and efficiency, and last, questions tied to the impact of these tools on the professional identity of bankers.

First, the very principle of recourse to profiling is questioned inasmuch as it necessarily relies on an abstraction inferred from behaviour, either actually observed or deemed possible. Profiles are based on the correlation of data supposedly characteristic of a model identifying a person, organisation or practice. They are therefore totally dependent on the quality and relevance of the information on which they rely. Financial intelligence has certainly developed considerably over the last two decades, and profiling is a way of optimising the use of scarce resources. But to the minds of many users, neither the compiling of a maximum number of cases nor the excellent ability of computer software to establish correlations between scattered facts provide an absolute guarantee of the validity of profiles. Specialists in these tools also point to an inflationist trend in data collection. Initially, profiling only used the data required to decipher transactions, but its field of action has gradually been extended considerably. There has been a tendency to maximise information-collection, which may now include personal information and be used for marketing, security reinforcement and/or client behaviour-analysis purposes. As one compliance officer says, « It has a Big Brother side. You know everything about your client, but what do you do with all that information? ».

This accumulative dynamic is reinforced by a tendency of profiling to move from a mere synthetic description of the past to attempted predictions, exemplified by client risk-scoring. This increased centralisation of intelligence has led some professionals to wonder about the consequences of these practices for such values as confidentiality in the banking profession, and sometimes, more broadly, for civil rights. The subject is much more controversial in the Anglosphere

[1] The EU list actually only contains thirty organizations and twenty-six individuals.

[2] CANHOTO A.I., 2007, *Profiling Behaviour: the Social Construction of Categories in the Detection of Financial Crime*, London, London School of Economics and Political Science, Department of Management; WEBB L., 2004, A Survey of Money Laundering Reporting Officers and their Attitudes Towards Money Laundering Regulations, *Journal of Money Laundering Control*, 7, 4, 367-375.

where profiling is viewed as possibly feeding discrimination among clients[3] and raising the broader issue of the protection of privacy, threatened by the present-day prospects of what is known as « dataveillance »[4].

The tremendous potential offered by these tools potentially raises the issue of threats to fundamental rights, as the Commission Nationale Informatique et Libertés (CNIL) (an independent administrative authority whose mission is to guarantee that the development of information technology would ever remain respectful of privacy, personal and public liberties) pointed out for France in a 2003 report. The report claims that these tools neglect personal data protection and that they do not refer clearly to the information technology and liberties regulations. According to the CNIL, while non-observance of the money laundering regulations « is criminally liable to punishment, non-respect of the rules pertaining to information technology and liberties is liable to penal punishment of equal severity »[5].

When the CNIL first appeared on the scene it apparently represented a source of tension between the requirements of the anti money laundering and terrorism financing normative framework on the one hand, and the protection of personal liberties, which is constantly being reinforced at both the French and European levels, on the other hand. However, its principles have gradually lost their bite: constraints on bank reporting were first alleviated in 2005, and further so in 2006-2007, while new decisions extended the modalities of intelligence-sharing – previously prohibited – within banking conglomerates, and made it easier to close accounts. The necessities of combating money laundering and above all of fighting terrorism are imperatives with which the CNIL was obliged to come to terms.

Those compliance officers, who are concerned about the climate of legal insecurity in which they work, claim to « fear » the CNIL and find it difficult to anticipate its demands and respond to them. One officer even compares it to a « blind spot ».

Defensible Compliance

Neither the increasing sophistication of tools nor the accumulation thereof has dissolved all the problems and doubts facing banking actors since they have been in charge of the fight against money laundering. Our research shows that the development of these tools does not rest on broad agreement as to their efficiency and their objective.

All things considered, there is something of a paradox in their widespread use in banking.

Our interpretation is that the apparent contradiction between the achievements of these instruments and the uncertainties they raise is dissolved by a shift in perspective: expectations with respect to them are not primarily what they officially claim to be, that is, accurate selectivity. Their efficiency for the banking institutions and their staff lies elsewhere: diligent use of these tools is above all a sign of compliance. Their use and the footprint they leave are there to show, concretely, that the establishment submits to public norms and to good professional AML practices.

In conclusion, the reason behind the brilliant career of these tools is less the safety they offer for client-related risks than the safety they provide in warding off public regulation. Information technology does not afford operational safety as much as the safety provided by « auditability »[6], « defensible compliance »[7], in the sense of a scheme aimed at protecting the institution against suspicion as well as one that may be assumed publicly.

Gilles FAVAREL-GARRIGUES
(*favarel@ceri-sciences-po.org*),
Thierry GODEFROY
(*godefroy@cesdip.fr*)
and **Pierre LASCOUMES**
(*pierre.lascoumes@sciences-po.fr*)

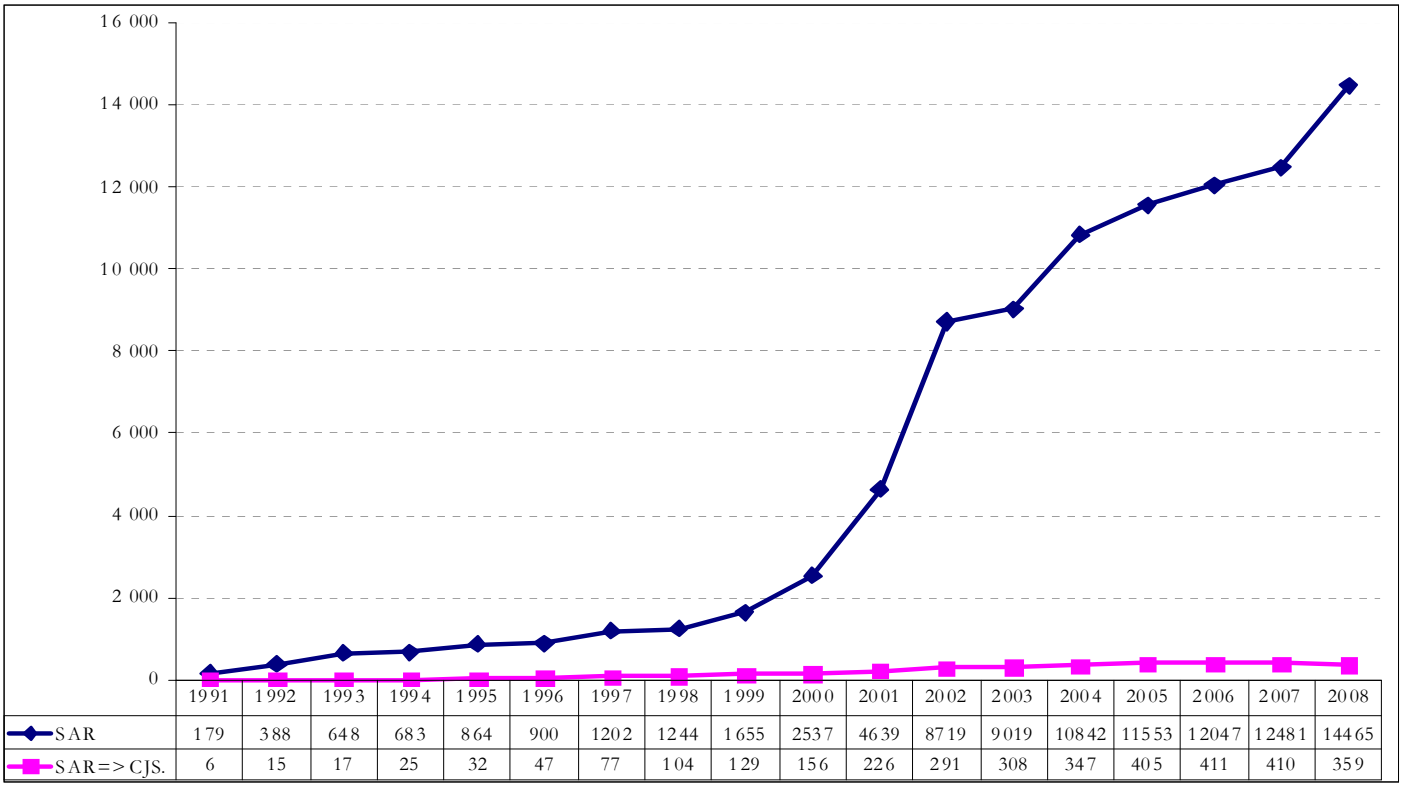
[3] SCHAUER F., 2003, *Profiles, Probabilities and Stereotypes*, Cambridge, Harvard University Press; HILDERBRANDT M., GUTWIRTH S., 2008, *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Dordrecht, Springer.

[4] LEVI M., WALL D.S., 2004, Technologies, Security and Privacy in Post 9/11 European Information Society, *Journal of Law and Society*, 31, 2, 194-220.

[5] CNIL, 2003, *La lutte contre le blanchiment d'argent et le financement du terrorisme au sein des organismes financiers : quels enjeux pour la vie privée de la clientèle bancaire ?*, october 7, session 10.

[6] POWER M., 1997, *The Audit Society : Rituals of Verification*, Oxford, Oxford University Press.

[7] As R. ERICSON terms it *in* Ten Uncertainties of Risk-Management Approaches to Security, *Revue Canadienne de Criminologie et de Justice Pénale*, 2008, 48, 3, 345-359.



	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
SAR	179	388	648	683	864	900	1202	1244	1655	2537	4639	8719	9019	10842	11553	12047	12481	14465
SAR=>CJS.	6	15	17	25	32	47	77	104	129	156	226	291	308	347	405	411	410	359

Figure 1: Trends in Suspicious Activity Reporting and Referrals to Criminal Justice System (Source: TRACFIN)