Stashing the cash: banks, money laundering and the battle against illegal logging

Reflections from Fern

Mark Gregory
September 2015

Acronyms

AML	anti-money laundering
AMLD	Anti-Money Laundering Directive
BBA	British Bankers' Association
CDD	Customer Due Diligence
CITES	Convention on International Trade in Endangered Species
CSR	Corporate Social Responsibility
EDD	Enhanced Due Diligence
EIA	Environmental Investigation Agency
EU	European Union
FATF	Financial Action Taskforce
FIU	Financial Intelligence Unit
FLEGT	Forest Law Enforcement, Governance and Trade
JMLSG	Joint Money Laundering Steering Group
KYC	'know your customer'
NGO	non-governmental organisation
OECD	Organisation for Economic Cooperation and Development
PEP	politically exposed person
UNCAC	United Nations Convention against Corruption
UNODC	United National Office on Drugs and Crime

Executive Summary

Illegal logging is believed to account for between 15% and 30% of the international trade in timber. Revenues from timber crime are likely to run into billions of dollars each year. Data such as this has prompted the European Union (EU), the World Bank and others to call for tougher enforcement and more effective use of anti-money laundering (AML) procedures as a way of tackling the illicit financial flows that support illegal logging.

Against this background, Fern carried out research to find out if action on money laundering could be a worthwhile lever to help preserve the world's forests.

We were interested in two issues in particular. First, should forest crimes be made a predicate offence under the EU's Anti-Money Laundering Directive, and would this make it easier to bring prosecutions? Second, how do European banks implement AML rules, and would it be worth trying to persuade them to pay special attention to the problem of money laundering linked to logging?

We looked at the framework of rules and institutions governing anti-money laundering, including the European Union's Anti-Money Laundering Directive, the Financial Action Task Force (FATF) – the international body established to combat money laundering and Financial Intelligence Units (FIUs), which each member country of the FATF is obliged to set up. We examined database tools such as World-Check, used by financial institutions to look for evidence of money laundering; and we looked at the issue of corruption in financial institutions and efforts to combat it. We also talked to experts and practitioners in banking.

We concluded that, while action on money laundering can in theory play a significant part in helping to preserve the world's forests, there are numerous obstacles:

• Making illegal logging a predicate offence under the AML Directive would be unlikely to change bank behaviour or make it easier to bring AML illegal logging cases to court.

• FIUs are overwhelmed by the quantity of 'suspicious transaction reports', and they do not have the resources to investigate more than a tiny proportion – mainly in their priority areas of drug dealing and serious organised crime. In this context, it is unlikely that illicit dealings related to illegal logging will receive much attention.

• FIUs are reluctant to investigate AML in other jurisdictions unless requested by authorities in those jurisdictions. This means that EU-based FIUs, for instance, would be unlikely to investigate money laundering in the major timber-producing countries.

• Illegal logging is difficult to detect merely by looking at cash flows, as illegal transactions look remarkably like legal ones.

• Finally, there is little evidence that revenues from illegal logging flow to Europe on a significant scale, making it more difficult to make a case for reforming EU money laundering procedures.

Illegal logging and money laundering remain important issues, which can and must be tackled, but it is doubtful that linking the two would be a very effective way forward, although there are clear cases where it has worked.

The context

Although there are no definitive statistics on the value of the trade in illegally sourced timber globally, the opening paragraph of the World Bank study 'Justice for forests' gives this estimate:[1]

'Every two seconds, across the world, an area the size of a football field is clear-cut by illegal loggers. In some countries, up to 90 per cent of all the logging taking place is illegal. Estimates suggest that this criminal activity generates approximately US$ 10–15 billion annually worldwide – funds that are unregulated, untaxed and often remain in the hands of criminal gangs.'

Comparable estimates come from other sources. Interpol has this assessment of the scale of the numbers involved and the environmental consequences:[2]

'It is estimated that illegal logging accounts for 50–90 per cent of the volume of forestry activities in key producer tropical forests, such as those of the Amazon Basin, Central Africa and Southeast Asia, and 15–30 per cent of all wood traded globally. ... Clearly, if left uncontrolled, illegal logging will undo the global community's efforts to reduce carbon emissions from deforestation and forest degradation. In addition to the environmental damage, the trade in illegally harvested timber is highly lucrative and estimated at least at USD 30 billion annually.'

A central problem has been the failure of criminal justice systems within some timber producing countries to penalise offenders or deter future abuses. According to the World Bank:[3]

'Forest law enforcement has been found to be highly ineffective in most countries at deterring illegal logging. A four-year study conducted in four resource-rich countries (Brazil, Mexico, Indonesia, and the Philippines) found that the cumulative probability of an illegal

[1] Goncalves MP, Panjer M, Greenberg TS, Magrath WB, 'Justice for forests: improving criminal justice efforts to combat illegal logging.' World Bank, 2012. http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/0,,contentMDK:23146160~pagePK:148956~piPK:216618~theSitePK:282885,00.html

[2] http://www.interpol.int/Crime-areas/Environmental-crime/Projects/Project-Leaf

[3] Ibid.

logging crime being penalized is less than 0.082%. In one of the regions examined (Papua, Indonesia) the cumulative probability of being convicted of illegal timber shipment was only 0.006%.'

With local enforcement of forest rules failing on such a catastrophic scale, there is pressure to find ways of tackling the problem through mechanisms that can operate outside the countries where the problems are taking place. This is a large part of the attraction of using anti-money laundering procedures. AML processes can potentially be applied at the international level or through the legal systems of timber-importing countries, as well as the countries where trees have been illegally felled. In other words, application of AML procedures on money flows linked to logging, passing through the global financial system could be a way of countering the inadequacy of forest law enforcement in timber-producing countries.

Like its legal counterpart, the trade in illegal timber is international in character. It flows across national boundaries, which may make it vulnerable to disruption by action taken in jurisdictions far removed from the forests.

There are good reasons why anti-money laundering could be a useful mechanism for combatting illegal logging. This study set out to find out how it works in practice.

Much of what we discovered came from informants based in Europe's leading financial centre, London. The combination of our interest in EU procedures, and the fact that much of our data comes from the UK, means this paper is inevitably UK and EU-centric. However, our conclusions may have relevance outside the EU.

Many of the anti-money laundering experts and practitioners who spoke to us did so on a confidential basis, and we do not have their permission to quote them. Therefore this paper is short on references, and should be seen as a scrapbook of information and insights, intended as a contribution to the debate.

What is money laundering?

Money laundering is the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin.[4] It commonly involves three distinct phases.[5]

1. *Placement*
Cash generated from crime is placed in the financial system. This is often the point when proceeds of crime are most apparent and at risk of detection.

2. *Layering*
Once the proceeds of crime are in the financial system, layering obscures their origins by passing the money through complex transactions. These often involve different entities such as shell companies and trusts, and can take place in multiple jurisdictions.

3. *Integration*
Once the origin of the funds has been obscured, the criminal is able to make the funds reappear as legitimate funds or assets. They will invest funds in legitimate businesses or other forms of investment. Typically, this is the most difficult stage of money laundering to detect. Laundered funds may be reinvested in almost any type of asset from property to shares and bonds, and even gambling chips at casinos.[6]

The concept of the predicate offence is important in money laundering. The term refers to the underlying criminal activity that gives rise to the illicit proceeds that are later disguised. For the crime of money laundering to occur, a predicate offence has to take place first.

What constitutes a predicate offence varies between jurisdictions[7]. In some jurisdictions, all "serious" crimes or crimes carrying a penalty above a certain threshold (e.g. a year or more in prison) are regarded as predicate offences. In others, a list is made of particular crimes which constitute predicate offences. Financial transactions related to crimes that do not feature on the list cannot give rise to the offence of money laundering. Another approach used in some jurisdictions is to define as predicate offences all "acquisitive" crimes. Acquisitive crimes are offences that create proceeds (flows of money or goods).

In practice, most serious crimes – including drug trafficking, terrorism, fraud, robbery, arms trafficking, bribery and corruption – are seen as predicate offences in most jurisdictions.

Money laundering is a clandestine activity, which by its nature is hard to quantify. However, the UN Office on Drugs and Crime has estimated that the value of laundered funds was 2.7

[4] For further information see the UK Financial Conduct Authority's money laundering page: https://www.fca.org.uk/firms/being-regulated/meeting-your-obligations/firm-guides/systems/aml

[5] For further information see the UK Law Society's Practice Note on Money Laundering, 2013: https://www.lawsociety.org.uk/support-services/advice/practice-notes/aml/introduction/

[6] Money laundering through gambling chips may involve an individual going to a casino and buying chips with illicit cash. The individual then plays often for a relatively short time. When the person cashes in the chips, they take payment in the form of a cheque from the casino or get a receipt so they can claim the proceeds as gambling winnings. Information from: National Drug Threat Assessment, a report from the US National Drug Intelligence Centre, 2005.

[7] Information drawn from training material produced by the UK's Chartered Institute for Securities and Investment: http://www.cisi.org/bookmark/WEB9/COMMON/LIBRARY/FILES/QUALIFICATIONS/EXTERNAL%20SPECIALISTS/MATERIALS/WORKBOOK%20PREVIEWS%20FOR%20IAIN_DELETE%20AFTER%20USE/CFC_ED2_PREVIEW.PDF

per cent of global gross domestic product – or US$ 1.6 trillion – in 2009.[8] A decade or so earlier, the World Bank reported that the aggregate value of money laundering could be in the range of 2–5 per cent of global GDP, or between US$ 590 billion and US $1.5 trillion in money values of the time (1998). To put this in context, US$ 590 billion was the size of the entire Spanish economy at that time.

Money laundering crimes relating specifically to the forestry sector include: cash from illegal logging deposited into local banks; transfer of payments for illegal timber to accounts abroad; and money from illegal logging already placed in a financial institution that is invested in other assets such as shares, bonds, property etc.

EU money laundering rules

Each country within the EU has its own laws and processes for dealing with money laundering. However, national arrangements must be in line with rules set at EU level in Brussels. This overarching EU-wide framework is defined by the EU Anti-Money Laundering Directive (AMLD). Individual Member States must transpose the AMLD into their own laws, but they have some discretion over the details of how this is done, and there is nothing to stop them from adopting tougher rules than the minimum standard set by the Directive.

The AMLD has been revised several times. The first money laundering directive, adopted in 1991, focused mainly on money flows associated with drugs crime going through traditional financial institutions such as banks. Subsequent iterations of the AMLD have expanded the range of money laundering crimes and broadened the scope of which institutions and people are obliged to look out for money laundering – to include, for example, lawyers, notaries, accountants, estate agents, art dealers, jewellers, auctioneers and casinos as well as banks.

At the time of writing (July 2015) the rules are in transition, with the third directive – Directive 2005/60/EC of 26 October 2005 – in the process of being replaced by the fourth directive – Directive 2015/849 of May 2015. The fourth directive[9] took legal force in June 2015. EU Member States must transpose its requirements into national laws within two years.

The third money laundering directive set up a system based on Customer Due Diligence (CDD) for banks and others obliged to look out for money laundering, also referred to as a risk-based approach. An often-mentioned acronym is KYC – 'know your customer'. KYC is all about understanding the client sufficiently well to be able to identify the level of risk of them being engaged in money laundering – and then, based on that understanding, to put the appropriate level of AML risk management in place.

[8] Data in this paragraph comes from the website of the Financial Action Taskforce, an inter-governmental body with oversight over anti-money laundering processes: http://www.fatf-gafi.org/pages/faq/moneylaundering/
[9] For the text, go to: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.141.01.0073.01.ENG

The third directive established two tiers of CDD: (1) Simplified Customer Due Diligence, for most types of transactions and customers, where generally the money laundering risk is low; and (2) Enhanced Due Diligence, which applies to situations where there is a higher risk of money laundering, e.g. where the customer is not physically present for identification purposes; cross-border banking relationships with customers or institutions in other countries; and financial relationships with 'politically exposed persons' (PEPs).[10]

Experts consulted by Fern made a number of points about how the obligation on banks to conduct Customer Due Diligence applies to dealings with corporate clients in situations that could be relevant to timber-related money laundering:

- A key 'know your customer' moment is when an individual or business entity opens an account. Banks are obliged to establish the real identity of their clients.

- Banks must maintain a basic level of ongoing AML monitoring over their customers. With a corporate client, they are obliged to know roughly the nature of the business involved and to build a profile of the flow of funds, so they are able to spot any unusual activity. For example, a Thai company might routinely have dealings with suppliers in Indonesia and customers in Europe, but then makes a significant payment to somewhere else, such as the Cayman Islands. Its bank is required to have adequate systems in place to pick that up as an unusual and potentially suspicious transaction. The bank is then obliged to file a suspicious transaction report to the relevant authority, the FIU (see pages 13 to 15 for more information on FIUs and other anti-money laundering institutions). The bank is not generally obliged to do anything else, like stop the transaction, close the account or call the police. The bank is not required to make the information public.

- With Enhanced Due Diligence, banks are required to exercise additional vigilance and make extra checks in situations where there is especially high risk of money laundering. For example, they would be expected to keep and maintain lists of countries and areas of business where corruption is rife.

- Transactions involving politically exposed persons – individuals with high levels of influence, such as public officials, politicians and their close associates – are likely to be an especially important area of enhanced money laundering risk for timber crime. The exact definition of a PEP, and how PEPs should be monitored, is seen as very significant in the debate about AML and illegal logging.

- AML rules do not only apply to banks. They also apply to lawyers, accountants and other professionals involved in transactions. Estate agents and casinos

[10] PEPs are defined in the Directive as 'natural persons who are or who have been entrusted with prominent public functions and immediate family members or persons known to be close associates of such persons' (Article 3.8).

are also covered (laundered funds often end up in property or gambling). These 'intermediaries' often play a key role in money laundering. Laundering typically involves a complex chain of events and transactions. From a campaigning or investigating point of view, the corrupt lawyer or accountant in London or Paris, say, who handles the funds can be easier to take action against than a senior figure in business or politics in a timber-producing country whose money is being laundered.

Most of the above still applies under the fourth money laundering directive which came into force in June 2015. Member States must incorporate its terms into national laws within two years. The new directive is less prescriptive than the old one, which was criticised by some banks, and others required to implement it, as over-bureaucratic and ineffective.

The new directive gives more flexibility to Member States as to how risks are defined and in deciding the scale of due diligence required – especially of smaller companies or individuals in low-risk situations.[11] It also extends the definition of predicate offences that can give rise to money laundering to include tax offences, and establishes new standards of disclosure on beneficial ownership of trusts and other assets – potentially making money laundering cases easier to investigate.

Making illegal logging an EU predicate

One of Fern's objectives in carrying out research into money laundering was to find out if there was any value in campaigning for forestry crimes to be specifically mentioned as predicate offences under EU money laundering rules. Many activities likely to be involved in forest crime are already predicate offences in most jurisdictions. For example, illegal logging typically involves an element of bribery and/or corruption at some point in the chain. Thus, it only makes sense to pursue the idea of making forestry crimes predicate offences in their own right if it leads to action on money laundering that could not or would not have happened using already existing predicate offences.

We are not the first people to look into this issue. Anti-money laundering has featured in official EU policies to combat illegal logging since 2003. In that year, the European Commission published its Action Plan for Forest Law Enforcement, Governance and Trade (FLEGT). The Action Plan aims to ensure that all wood imported and used in the EU is legally sourced. It combines measures in producer and consumer countries to facilitate trade in legal timber, and eliminate illegally sourced timber from the EU. It focuses on seven broad areas.

Money laundering came under area six: Use of existing legislative instruments. The objective was to harness money laundering (and other) legislation to combat the problem of illegally harvested timber and products derived from illegal timber coming into the EU. The Action Plan envisaged that this could be achieved by adapting EU-wide and individual member

[11] Numerous law firm websites analyse the details of the new AMLD, including Pincent Masons: http://www.out-law.com/en/articles/2015/june/new-eu-anti-money-laundering-rules-to-take-effect-from-26-june/

state money laundering rules and processes to facilitate prosecutions for timber-related financial crime in European courts. Specifically, under the original Action Plan, the European Commission agreed to:

- undertake work to establish the extent to which existing Member State legislation for money laundering is applicable to forest sector crimes, and disseminate this information widely to banks, financial institutions, financial crimes units and non-governmental organisations in the EU;

- encourage states to designate illegal logging as a crime for the purposes of the EU Directive on money laundering;

- provide development cooperation assistance, where appropriate, to strengthen developing country capacity to deal with forest-related money laundering issues; and

- encourage information-sharing between financial crimes units of the EU Member States on forest-related crimes.

The governments of two Member States, Britain and Germany, took the lead in following up the money laundering element of the Action Plan, with additional input from the European Commission. The effort was rapidly abandoned. Within two years or so of the Action Plan being launched, attempts to activate the section on money laundering had effectively ceased.

The reasons were set out in a document published several years later. The FLEGT Action Plan Progress Report 2003–2010[12] evaluated progress made in achieving all the targets laid down in the Action Plan over the first few years of operation, including money laundering.

One point to emerge was that few Member States had shown any real interest in pursuing AML as a strategy against illegal logging. Only six Member States (Bulgaria, Finland, Germany, Latvia, the Netherlands and the UK) had reviewed the application of money laundering or similar domestic legislation to forest crime in response to the FLEGT Action Plan. Several of those Member States were reported to have found that in theory they were able to bring timber crime prosecutions under existing national money laundering rules.

However, two said that prosecutions were difficult in practice due to the difficulty of gathering evidence and the existence of other priorities for prosecution staff. Based on a review carried out by Chatham House of the work conducted by Member States, the European Commission concluded that, even if it was in principle possible to address forest crime through domestic money laundering legislation, this was not the most useful option for advancing the aims of FLEGT.

Four Member States (Finland, Germany, Netherlands and UK) had tried to engage financial institutions, law enforcement agencies and other stakeholders in their jurisdictions on applying AML rules to logging cases, with Germany being the most active. Workshops were

[12] Hudson J, Paul C, FLEGT Action Plan Progress Report 2003–2010, January 2011: ec.europa.eu/europeaid/sites/devco/files/report-progess-2003-2010-flegt-20110126_en.pdf

held and the results disseminated. Additionally, the European Commission provided some technical and financial assistance to timber-producing countries intended to boost the implementation of forest related anti-money laundering processes outside the EU.

One Member State looked into using customs legislation to prevent illegal timber entering the market, but concluded that customs authorities were not mandated to enforce foreign laws. One country suggested investigating how FIUs around the world could be better informed and better equipped to fight timber-related money laundering.

The Progress Report says that the possibilities of assimilating the involvement of EU-based banks in financing illegal logging activities related to money laundering require further investigation. However, it also comments that '*generally speaking ... there seems relatively little interest in doing further work in relation to this component'.*

Fern took the view that the Action Plan's provisions on money laundering had been abandoned too readily. In 2014 we looked at the issue again, but from a different angle. While the Action Plan focused primarily on the potential for individual Member States to make more use of existing national legislation, or to adapt that legislation, to pursue logging-related money laundering cases, Fern looked into the possibility of reforming money laundering rules at the EU level.

As explained in an earlier section, individual member countries have their own money laundering laws and procedures but these national processes must be in line with the framework laid out at EU level in the EU's Anti-Money Laundering Directive (AMLD). Fern looked into whether activities associated with illegal logging should be made specific predicate offences in the EU AMLD. We thought it might be worth doing this for two reasons: (1) to force individual Member States to change their national laws if necessary; and (2) to draw attention to illegal logging as a significant issue in money laundering.

In the end, however, we concluded that efforts to include timber offences directly into the AMLD were unlikely to work for the following reasons:

- The AMLD refers to broadly defined categories of criminal activity. A list of very specific timber offences would seem out of keeping with this, and thus would be unlikely to be adopted.

- It was unclear if reform in the AMLD would actually lead to significant changes in anti-money laundering practice in Member States. There are some important differences in the legal systems of different Member States. We were advised that making logging offences predicate for money laundering under the AMLD might, for example, have some impact on German law but probably not on UK law. It was clear that a lot more detailed research would be needed to clarify the actual impact of changes in the AMLD in individual Member States.

- There were other general reasons (not related to the specifics of EU law) for thinking that anti-money laundering is unlikely to be a fruitful way of combatting illegal logging. These are set out later in this report.

The organisations involved in AML, its rules and institutions

Different countries have their own laws and procedures for dealing with money laundering. However, almost every country works within a framework of guidelines set by an international body called the Financial Action Taskforce (FATF). The rules applying within the EU, as described in the previous section, are derived from (but are not identical to) the FATF's guidelines. Other important players include Financial Intelligence Units (FIUs) and national financial regulators.

The FATF

The FATF was founded in 1989 on an initiative of the G7 to develop a coordinated response to money laundering at a time when this was perceived to be a growing international problem. Its first task was to draw up a set of guidelines, initially known as the 40 Recommendations, to advise governments on how to tackle money laundering. In 2003, in the wake of the 9/11 attacks on the USA, its mandate was extended to include terrorist financing. The FATF's objectives are '*to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system*'.[13]

The FATF has a small staff or secretariat of around 20 people located in the same building as the Organisation for Economic Cooperation and Development (OECD) in Paris. Ultimate decision-making power rests with the FATF's members. The FATF has 36 members, made up of 34 countries and two regional associations.

The FATF publishes information on best practice in AML procedures, and issues 'typologies': investigations into new or rising areas of AML concern that pose unusual or new problems. Recently it has done work on mobile payment systems and mobile banking done over the internet.

The FATF has also published a typology of the diamond sector – money laundering associated with conflict diamonds[14] – and it has issued a typology of 'hawala', the verbal money transfer system used by Somalis, which is seen as a conduit for terror finance.[15] An obvious campaign goal would be to build the case for a typology covering illegal logging.

The FATF does not deal with individual financial institutions; instead it issues recommendations to the relevant authorities in the countries that belong to it. These authorities – national financial regulators and in-country FIUs – are tasked with implementing the recommendations, enforcing AML laws and dealing with financial institutions in their own jurisdictions.

More information on the Financial Action Taskforce is set out in Box 1.

[13] http://www.fatf-gafi.org/pages/aboutus/
[14] Money laundering and terrorist finance through trade in diamonds, October 2013: http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf
[15] The role of hawala and other similar service providers in money laundering and terrorist finance, December 2013: http://www.fatf-gafi.org/documents/documents/role-hawalas-in-ml-tf.html

Box 1: The FATF

People close to the Financial Action Task Force told Fern that the organisation is aware of a possible link between illicit money and illegal logging. However, this has been hard to prove.

To make illegal logging a specific priority in anti-money laundering, the FATF would want evidence of characteristic patterns of money laundering transactions relating very directly to illegal logging. In many cases, the processes of laundering the proceeds of timber related crime are likely to be similar to those involved in laundering the proceeds of many other types of crime. For money laundering in illegal logging to be singled out for special attention, we were told, it would be necessary to demonstrate that there was something distinctive or unusual about the transactions involved that distinguished it from other areas of crime.

FATF guidelines already refer to "environmental crime" as a potential category of predicate offence (meaning that handling the proceeds may constitute money laundering). However, for years this provision attracted little attention and what constituted environmental crime seems not to have been defined. This may be about to change. One of the FATF's observer bodies, a regional grouping of mainly francophone countries in central Africa, is working towards a typology of environmental crime there. The grouping known by its French acronym, GABAK, includes Chad, Central African Republic, Equatorial Guinea, Gabon, Congo-Brazzaville and Cameroon. The principal focus is poaching but the exercise may also be relevant to illicit revenues from forest crime.

One of the FATF's responsibilities is to review the AML procedures of individual countries. In the past this has mainly been about technical compliance, but the current round of evaluation is now focusing for the first time on how effectively countries have tackled money laundering. The results are likely to be highly controversial. The only results published so far relate to Belgium. Belgium was found to have the core aspects of an effective AML system in place, although some elements were not in line with the FATF's latest recommendations.[16]

A measure of the FATF's influence is the attention given to the 'blacklist' it publishes of countries that have failed to implement its recommendations. Being labelled by the FATF as non-compliant has consequences. Individuals and businesses in those countries face difficulties in accessing the international financial system. Essentially banks are required to apply enhanced due diligence to every single transaction coming out of a blacklisted country. It is also seen as a public humiliation for governments, a threat of pariah status, which in several past instances has goaded them into action on AML. For example, Indonesia introduced its first AML laws in 2002 directly in response to the threat of being blacklisted.

[16] Anti-money laundering and counter terrorist financing measures in Belgium, Fourth round mutual evaluation report, April 2015: http://www.fatf-gafi.org/topics/mutualevaluations/documents/mer-belgium-2015.html

Financial Intelligence Units

Financial Intelligence Units (FIUs) are another important part of the AML institutional framework. Every member country of the FATF is obliged to set up an FIU. It is their job to monitor the implementation of AML procedures. They collect intelligence and pass it on to the FATF and to law enforcement agencies in the countries where they are based. A substantial part of their job is to analyse and act on suspicious transaction reports. For instance, if a bank has reason to suspect a potential money laundering operation, it is legally obliged to tell the relevant FIU by filing a suspicious transaction or activity report.

FIUs work together through an informal forum called the Egmont Group, which describes its role in the following terms:[17]

'Recognizing the importance of international cooperation in the fight against money laundering and financing of terrorism, a group of Financial Intelligence Units (FIUs) met at the Egmont Arenberg Palace in Brussels, Belgium, and decided to establish an informal network of FIUs for the stimulation of international co-operation. Now known as the Egmont Group of Financial Intelligence Units, Egmont Group FIUs meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the areas of information exchange, training and the sharing of expertise.'

The Egmont Group is currently composed of 139 member FIUs.

How banks check for money laundering

All banks within the EU work within the same basic set of rules on AML, and their actions are shaped by the same set of pressures. A number of our interviewees took the view that the key drivers for banks on AML are regulatory risk and the potential for reputational damage. Banks do not like being involved in scandals, and prefer to stay on the right side of the financial regulator for the jurisdiction (usually the nation state) they are in. Failure to do so can lead to large fines and, more significantly, damage to their standing with clients and other players in the financial sector. Nobody wants to be labelled as a rogue bank.

We were told that the main motivator in administering AML procedures is 'to stay out of trouble'. One strategy for doing this is for individual banks to copy their peers:

'[Banks] broadly have the same approach and procedures (on AML) ... and they see safety in numbers. They are less likely to be hit by the regulators if they're doing the same as other banks,' said a senior figure at an industry representative body for financial markets based in London.

A number of our respondents were quite cynical about what drives bank behaviour on compliance: *'Fundamentally it's a giant box ticking exercise,'* said Timon Molloy, editor of Money Laundering Bulletin, a specialist publication for AML professionals.

[17] For more details, go to the Egmont Group website: http://www.egmontgroup.org/

Where there are differences between jurisdictions in the EU, it may be influenced by the varying degrees of enthusiasm for AML on the part of different national regulators. The view of some in London is that financial regulators in France and Germany take the topic less seriously than their UK counterpart, which means that banks in those countries are more lax in their procedures. This was a statement of opinion backed by no evidence.

A key component of AML procedures at banks is running lists of names through databases to make sure they are not dealing with people or entities covered by UN sanctions or other blacklists put out by relevant authorities. Day-to-day AML mainly involves combing through vast quantities of information – usually on computer databases – to look for specific things, e.g. individuals with criminal records, suspicious-looking transactions, opaque financial structures, transactions involving countries subject to sanctions and so forth.

Compliance officers do not spend their days contemplating concepts such as illegal logging. Instead, they are buried in reams of data hunting for very specific 'red flags' – industry jargon for small anomalies – that could signify AML risk.

In principle, these processes could be adjusted to look more thoroughly for suspicious transactions relating to illegal logging. However, to have any value this would need to go beyond generalities. It would need to be clear that the precise red flags are relating to forestry deals and how these are different from the things that banks are already looking out for in their checks for money laundering.

Implementation, we were told, is mainly about identifying the level of AML risk and then putting adequate procedures in place to deal with that risk. The test of success is less to do with whether money laundering was stopped, or whether anyone was caught, than with whether an appropriate process was in place for the level of risk involved, and whether it was implemented properly. Banks stand to be fined by regulators for not monitoring clients and/or not collecting enough KYC information.

At the low end of the AML risk spectrum – a European citizen, say, applying to open an account or taking out a small personal loan at a European bank – banks apply a few simple standardised procedures such as looking at passports and other documents to verify the customer's identity, and running a credit check through automated databases, run by specialist ratings checkers like Experian and Equifax.

At the other extreme, in situations where AML risk is perceived to be extremely high – e.g. where a senior figure in a corruption-prone country wants to make a multi-million dollar deposit in a new account – the bank might even send in private investigators to check out the situation on the ground. However, only in exceptional cases would a bank be expected to go this far. Much more common is an intermediate level of checking that typically relies heavily on screening information held on various databases with computer software tools, backed up by layers of analysis by specialist AML compliance officers. World-Check is the best known and most widely used database, but there are many others, used for different purposes and with varying degrees of intensity depending on the perceived level of risk.

The broad test for triggering AML concern is that if an employee of the bank has a suspicion that the proceeds of a crime may be involved, they are legally obliged to report this. The report is then looked at by the money laundering department. They check the report against any other information they hold about the client. If it still looks suspicious, the report will then be passed on to a higher level for more intensive analysis. The report may go through several layers of scrutiny.

Once the bank has finally decided that there is cause for concern, it files a suspicious transaction report to the relevant FIU. It is up to the FIU to determine what, if any, further action should be taken. In Britain, the FIU is located within the National Crime Agency, a body with broad law enforcement responsibilities. Arrangements in other EU countries vary in detail but the broad picture appears to be similar.

As many as 350,000 suspicious activity reports[18] are filed each year in the UK alone.[19] There is no public information available on what happens to them all. With that volume of data it may be assumed that many are ignored. With resources limited and budgets under pressure, there are real concerns about whether FIUs have the capability to deal effectively with the flood of AML reports they receive. The situation is likely to be similar in other parts of the EU. This makes it questionable whether UK officials would give much priority to investigating suspicions of money laundering linked to forestry in faraway places. Their remit includes AML in the UK as well as overseas. It would not be surprising if they opted to focus scarce resources on, say, suspicious transactions involving drug dealers and organised crime in the UK, rather than goings-on half a world away in a tropical forested country. Again, the situation in other EU nations is likely to be similar.

Box 2: Case study of AML compliance at one bank (anonymised)

A conversation with a former 'senior change advisor' with a major European bank provided insight into the culture of AML compliance. Our source worked on e-training programmes to improve money laundering compliance standards at the bank.

The environment was described as 'like a factory' and 'a world of protocols and procedures'. The work involved looking for 'red flags' thrown up by churning data through very technical systems. The bank created lists of suspect individuals based on advice issued by the US government, the EU and others, along with 'blacklists' of countries. Our source never came across any mention of illegal logging but the training programmes did cover issues such as human trafficking and drugs crime. There was a lot of list-building, and comparing lists to other lists of people covered by US sanctions etc.

[18] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/specialist-capabilities/ukfiu

[19] Suspicious activity reports mostly relate to suspected money laundering but they are also used in the investigation of criminal activities such as benefit fraud, international drug smuggling, human trafficking and terror finance.

PEPs – politically exposed persons – featured highly in the system. Staff spent a fair bit of time compiling and analysing lists of PEPs, often using World Check as a reference point. Actions centred on PEPs were relatively straightforward. Staff also spent time profiling complex corporate structures in sectors of AML concern, which our source found very difficult to understand.

In the online training our source ran, one of the examples quoted as a 'red flag' that would trigger AML concern was the name Gadaffi. The system would throw up an alert at the mention of a name similar to that of the former Libyan dictator. All names similar to Gadaffi would get checked at the first level of defence as a matter of course and might go on to a second level for examination in more detail.

The bank had created two 'hubs' for AML analysis for its global operations – one in Europe, the other in South Asia. Our source was concerned that the analysis was being carried out by technical people who had little understanding of, or the context for, what they were dealing with – generally transactions and people many thousands of miles away.

Our source observed a cultural clash between 'front-office people', staff engaged with clients, who generally saw AML compliance as a nuisance, and 'back-office people', made up of support staff such as compliance analysts beavering away with their protocols and procedures.

The bank's tools: AML compliance databases

Due diligence risk databases are one of the main tools that financial institutions use to look for evidence of money laundering in their clients' transactions. The best known and most used is **World-Check**, a vast searchable database that is continually updated with information flowing in from thousands of different sources. All the information comes from publicly available sources.

These sources include US and other government agencies, international bodies such as the UN, Interpol and Europol, and media reports from news websites, newspapers and journals around the world (in several languages). Users arrange to receive alerts and updates on particular topics. They can also hunt for information in ways similar to carrying out a very elaborate Google search. World-Check is owned by Thomson Reuters, the group that runs the Reuters news agency, and which supplies financial data to traders on global financial markets.

Since World-Check was founded in 2000, increasingly sophisticated software tools have been developed to help users identify and analyse the information they want and to enable them to crosscheck vast streams of data against other datasets.

World-Check is the most widely used and best known service of its type in AML. However, it has various competitors that operate in similar ways, but which may be more specialised. These include:

LexisNexis, whose AML compliance database has a legal focus and which is popular with lawyers working in AML. It has various different products including software for high-speed checking of PEPs.

Dow Jones Risk Compliance, which are similar to World-Check.

Dun and Bradstreet is a big name in many areas of business information. Its AML product is focused on helping banks untangle the complex web of opaque corporate structures that often go with money laundering. For example, it provides information that may help identify the beneficial owners of shell companies.

Bureau van Dijk also focuses on corporate structures.

Others include **Accuity** and **Global Screening Solutions**.

> Box 3: LexisNexis Diligence: an example of a risk screening database
>
> LexisNexis Diligence draws on huge amounts of constantly updated information; 175,000 new documents are added to the database every day. Each document is tagged with subject headings which enables identification in searches. Types of data include the latest updates from international agencies, US government and so forth. But there is also a large element of screening media sources. LexisNexis has licensing arrangements with 4,000 publishers of newspapers, journals, news websites and other organisations, covering national and local publications all round the world, along with specialist journals etc. If something appears in a local newspaper, say, in a remote part of Indonesia, it will immediately appear on their database if the publication has an online presence. They do not directly access NGO reports but if, for instance, Greenpeace publishes a study or issues an alert, it will get into their database if it gets reported by a newspaper or journal somewhere.

Uses of AML databases

AML databases are used for a wide variety of purposes. For example, bank staff may consult databases to find out if people involved in transactions are mentioned on lists of Politically Exposed Persons and therefore require higher levels of due diligence. Checks are also made against lists of individuals subject to sanctions or alerts by bodies such as law enforcement agencies, the US government and the UN.

One key tool is what is referred to as 'negative media screening', which involves looking to see if individuals or organisations that banks are doing business with have been subject to adverse comment in the news media. Names are checked against lists of pre-defined 'derogatory' terms. These terms can consist of any word or phrase, so in AML searches the chosen term might be 'corruption' or 'fraud', but it could be literally anything. The system

throws up an alert if the name appears within a pre-set number of words (perhaps fifty) of the chosen derogatory term. So, for example, if you wanted to see if the controversial former chief minister of Sarawak (Abdul Taib Mahmud) had been linked to illegal logging, you would run a check that would sift through millions of documents. The system would throw up every instance of publications anywhere in the world where the name Taib had been mentioned within fifty words of the term 'illegal logging'.

This process can throw up thousands of references, many of them irrelevant. Software analytic tools are then used to identify the important references and narrow down the data set that has to be sifted. Negative media screening is a frequently used tool for identifying AML risk.

While single searches on one person do take place, it is more common to process large datasets in batches. This involves running large numbers of names – possibly thousands or even millions – through the system, using software analytic tools to find connections or identify politically exposed persons whose activities may require additional checking.

Identifying PEPs, as part of Enhanced Due Diligence, is a major undertaking. There are commercial companies that make a living from compiling lists of PEPs.

Making AML a priority for banks

Bank AML is based on endlessly checking data from one source against data from other sources. It tends to focus on identifying points of detail that suggest specific causes for concern rather than broad themes. The emphasis tends to be on processes rather than outcomes, but even by this measure the track record is not particularly good. A 2011 report by the British financial regulator on how UK banks handle situations with high money laundering risk found severe weaknesses in the application of procedures relating to high-risk clients, PEPs.[20] An excerpt from the report's conclusions is reproduced below:

'Some banks appeared unwilling to turn away, or exit, very profitable business relationships when there appeared to be an unacceptable risk of handling the proceeds of crime. Around a third of banks, including the private banking arms of some major banking groups, appeared willing to accept very high levels of money-laundering risk if the immediate reputational and regulatory risk was acceptable. Over half the banks we visited failed to apply meaningful enhanced due diligence (EDD) measures in higher risk situations and therefore failed to identify or record adverse information about the customer or the customer's beneficial owner. Around a third of them dismissed serious allegations about their customers without adequate review. More than a third of banks visited failed to put in place effective measures to identify customers as PEPs. Some banks exclusively relied on commercial PEPs databases, even when there were doubts about their effectiveness or coverage. Some small banks unrealistically claimed their relationship managers or overseas offices knew all PEPs in the countries they dealt with. And, in some cases, banks failed to identify customers as PEPs even when it was obvious from the information they held that individuals were holding or had held senior public positions. Three quarters of the banks in our sample failed to take adequate measures to establish the legitimacy of the source of wealth and source of funds to be used in the business relationship. This was of concern in particular where the bank was aware of significant adverse information about the customer's or beneficial owner's integrity.'

[Note: Since Fern completed the research for this report, the UK government has issued a national risk assessment of money laundering. The Treasury and Home Office report warned that the UK's banking, accountancy and legal services sectors were at a high risk of exposure to handling corrupt money, with the financial sector facing "significant intelligence gaps, in particular in relation to 'high-end' money laundering.]

At some levels banks seem open, indeed almost eager, to engage with NGOs and to be alerted to new issues. That was certainly the message we got from talking to the British Bankers' Association (BBA), the industry body for UK banking. The association sees itself as very 'proactive' and is 'happy to meet with NGOs', claiming 'there's been a lack of dialogue'. The BBA described illegal logging as an area that the banks have 'an interest' in identifying and stopping.

They also claim to pay attention to UN publications and the work of some NGOs (they specifically mentioned Global Witness). The BBA said it works closely with the UNODC and

[20] Financial Services Authority, 'Bank's handling of high risk money laundering situations', 2011. www.fca.org.uk/static/documents/fsa-aml-final-report.pdf

Europol. The BBA mentioned several banking industry forums that influence day-to-day AML processes at individual banks. General guidance for banks comes from the Joint Money Laundering Steering Group (JMLSG). It has high-level government involvement, and includes representatives from banking organisations.

The BBA also says that banks would take forestry AML more seriously if there was clear evidence of the proceeds of illegal logging being laundered. They want hard data, along with methodologies and risk analysis reports.

However, others we spoke to gave a more cynical assessment of how seriously banks take AML compliance. Here are some quotes from a senior figure in a financial markets representative organisation:

'People at the top (of banks) have lofty ideals but these don't translate to the coal face.'

'Unless they're getting regulatory pressure, they won't do anything.'

'*If you have to spend money (on thorough checks and procedures), people won't do it.'*

However, we were told that the status of compliance officers has improved markedly in recent years. It appears that AML compliance is taken a lot more seriously within banks than was the case even five years ago.

While we did come across some willingness among banks to take AML and illegal logging seriously, the obstacles to making much progress in practice still seem formidable.

A new emerging area: supply chain and anti-corruption compliance

Due diligence associated with money laundering risks is only one of several forms of due diligence used by banks and other financial institutions. This section looks at some of the other types of due diligence, to see if they might have a role in combatting illegal logging.

Corporate Social Responsibility

AML compliance procedures tend to concentrate on very specific risks. They are not set up to deal with broad ethical concerns. But there is a newly emerging area of compliance: Corporate Social Responsibility (CSR), which could play a part in areas such as illegal logging. For example, LexisNexis runs a database product, **Smartwatch**, to enable supply chain managers to identify political, economic, social and ethical risks that could disrupt their business or damage their company's brand.

LexisNexis clearly sees a market opportunity in this area driven by tougher regulatory frameworks – e.g. the Dodd-Frank reforms in the US (prompted in part by the global financial crisis) and the 2010 Bribery Act in the UK – and increasing awareness by companies of the risks of reputational damage from social and ethical concerns.

Increasingly, corporations do not want to run the risk of doing business with people who might embarrass them (by turning out to be employers of child labour, killers of baby seals or wreckers of rainforests). Smartwatch is a searchable database that helps them identify such risks and avoid them. There are numerous similar competing products. We were told that supply chain data products are so far more established in the US than in Europe. In the US, companies are under pressure to clean up their supply chains partly in response to Dodd-Frank but also state-level legal moves. For instance, the California Transparency in Supply Chains Act of 2010[21] requires large retailers and manufacturers doing business in the state to disclose what steps they are taking to eradicate slavery and human trafficking from their supply chains.[22]

Corruption as a compliance issue

Corporate compliance departments do not simply look for evidence of money laundering. They may also check clients and business partners for association with other risks for which they are required to carry out due diligence, such as violations of UN sanctions against countries such as Iran or Syria, corruption or links to terror finance. Campaigners have tended to look to due diligence connected with anti-money laundering as providing a way of getting at money flows linked to timber crime. However, it may be that some of the other areas of required due diligence could be more effective than AML in providing potential leverage points.

[21] This document from the California Department of Justice explains it well: http://oag.ca.gov/sites/all/files/agweb/pdfs/sb657/resource-guide.pdf

[22] More precisely, the Act requires every retail seller and manufacturer doing business in California and having annual worldwide gross receipts that exceed $100 million to disclose its efforts to eradicate slavery and human trafficking from its direct supply chain for tangible goods offered for sale. For a commentary, see for example http://www.pillsburylaw.com/california-transparency-in-supply-chains-act

One senior figure we spoke to at a compliance database company said he thought that logging transactions could be made a higher priority in AML compliance at banks, but only if there were sufficient new sources of data available on timber deals to flag up specific money laundering risks. He reckoned it would be easier to get traction for illegal logging as a compliance issue through raising the profile of the topic on databases relating to other types of due diligence (such as CSR, supply chain management and anti-corruption). He also made the point that AML compliance and anti-corruption compliance are handled increasingly by the same departments in banks.

Banks, it seems, are coming under pressure from two different directions. The Financial Action Taskforce (backed up by national financial regulators and the EU AMLD) is pushing them to do better on money laundering. Meanwhile, quite separately, bodies like the UN and OECD are driving them to improve their performance on tackling financial flows linked to corruption.

The United Nations Convention Against Corruption (UNCAC) has created an international legal framework that has prompted banks and companies to take corruption seriously as an issue. Meanwhile, the OECD has had an influential role in formulating the guidelines and fostering the debate. A number of the people we spoke to suggested that anti-money laundering compliance and anti-corruption compliance are in a sense converging, with organisations looking to deal with both types of risk using the same staff and similar procedures. Banks and businesses are also being forced to engage more seriously with corruption as an issue through changes in national legislation. In Britain the Bribery Act 2010 has imposed much tougher requirements on UK banks and businesses, and the first prosecutions have recently come to court. Equivalent processes are happening in other EU Member States.

Why AML is not a useful tool against illegal logging

Fern started this research with two broad questions in mind. First, could reform of EU money laundering rules through adding explicit provision for timber-related financial crime have the effect of bringing more forestry money laundering cases to court? Second, are there any steps that can be taken to ensure that banks and other financial institutions make timber crime a higher priority in the way they administer AML procedures? Sadly, we concluded that it would be difficult in practical terms to make effective use of AML as a lever to tackle illegal logging on either front. How we came to this view is summarised in the bullet points below.

- Our scoping research suggested that amending the EU Anti-Money Laundering Directive (AMLD) to make illegal logging a predicate offence would have little practical impact in changing bank behaviour or making it easier to bring AML illegal logging cases to court.

- There are some crucial flaws in the way the system works which make AML procedures of doubtful value. If banks suspect money laundering, they are merely required to file a suspicious transaction report to the relevant Financial Intelligence Unit (FIU). FIUs are often overwhelmed with these reports; 350,000 were filed in the UK alone in 2013. FIUs do not have the resources to investigate more than a very small proportion.

- FIUs historically have not regarded illegal logging as a major AML priority. They tend to focus their limited resources on areas such as drug dealing and serious organised crime. Unless this changes (which seems unlikely), banks will feel little pressure to get serious about AML and forests.

- FIUs usually only investigate AML in other jurisdictions when there is specific reason for them to do so – e.g. a court case in a timber-producing country or a request from a timber-producing country. This is a major drawback which undermines one of the principal arguments for using AML as a tool for tackling timber crime. AML has been proposed as a way of tackling criminal activity through action in the international arena that is not being dealt with at local level in timber-producing countries, where law enforcement is poor. But this will not work if FIUs outside timber-producing countries refuse to take on cases that are not being investigated or acted on locally. It could be argued that the solution is to put pressure on FIUs outside timber-producing countries to behave differently: but Fern was told that the chances of achieving this behaviour change are remote. This judgement, of course, may be wrong. If FIUs could be persuaded to make financial transactions relating to timber crime that has taken place in other parts of the world a higher priority, AML could be an effective tool for tackling the issue of illegal logging.

- It can be difficult in practical terms for FIUs outside timber-producing countries to investigate money laundering relating to logging. FIUs identify money laundering by looking for unusual patterns of transactions going through accounts. The problem with the timber trade is that illegal transactions look remarkably like legal ones. Illegal logging tends to be an 'inside job'. Companies with timber concessions log in places they are not

supposed to or otherwise break the terms of their permits. This is hard to pick up simply by examining money flows going through accounts. A common scenario for money laundering is a criminal gang attempting to conceal the illegal nature of the proceeds of crime. This may be the pattern for certain types of environmental crime – poaching and wildlife trafficking, for example – but it is not typical of illegal logging. Forestry is generally an industrial operation. A tree trunk is not something that can be easily hidden and smuggled unlike, say, an elephant tusk or rhino horn. The most likely scenario for large-scale illegal logging is not a criminal gang that enters a forest to 'steal' trees but rather a legitimate operator who has some tree felling operations that are legal and others that are not. In these circumstances, transactions relating to the criminal and non-criminal sides of the business may look similar, which means there may not be any obviously anomalous patterns of financial activity for bank investigators staring at computer screens thousands of miles away to pick up as indicators of money laundering. However, theft of extremely high-value and rare species of trees of the type covered by the CITES Convention – rosewood, for example – may involve outside criminal gangs, whose efforts to hide the proceeds do fit the classic money laundering mode.

- The UK and German governments (drawing on research conducted by Chatham House) came to similar conclusions on the value of toughening up European legislation when they investigated making use of AML procedures to curb illicit financial flows related to illegal logging in the mid-2000s. We spoke to several people involved in that initiative, which was a response to the section on AML in the FLEGT Action Plan (2003). The Action Plan called for further investigation of AML. The broad conclusion was that there was little to be gained from pursuing this further. This point is discussed in greater detail below.

- More fundamentally, there is little evidence that revenues from illegal logging of tropical forests flow to Europe on a significant scale. This undermines the case for making reform of EU money laundering procedures a priority. If illicit funds from tropical forest destruction come to Europe at all, it is likely to be as a final destination after the laundering process is complete – laundered funds may, for example, re-emerge as investments in European property or financial assets. At this late stage detection is usually difficult, though not impossible. Earlier stages in the process of hiding the proceeds of timber crime through money laundering – i.e. placement into the financial system and layering to conceal the criminal source – are more likely to take place in regional financial centres close to forests (e.g. Hong Kong or Singapore in the case of Asia) or offshore tax havens with banking secrecy, such as the British Virgin Islands. However, while Europe itself may not be centre stage for logging AML, it is possible that European financial institutions play a role, knowingly or unknowingly, in concealing the proceeds of timber crime through their operations outside Europe. If that is the case, it may be worth targeting through action in Europe. The first step would be finding evidence that European banks are involved in this way. Currently there is no such evidence, but that may be because nobody has seriously looked for it. We were told that the UK Treasury Department may be keen to find ways of encouraging British Overseas Territories to apply AML procedures more thoroughly – although it has no power to force them to do anything. They have their own legal systems. This point is of more than academic interest: two of the world's most notorious off-shore financial centres, the

British Virgin Islands and the Cayman Islands, are administered as British Overseas Territories.