

# A new front – IPR theft, money LAUNDERING and TERRORIST FINANCING

**The banking industry is exposed to significant risks of money laundering and terrorist financing of the proceeds of IPR theft. A new front is unfolding in the Global AML/CFT war. Rohan Bedi, author of the PricewaterhouseCoopers Singapore publication *Money Laundering Controls and Prevention* and senior AML implementation manager of a leading international bank, and Jonathan Dotan, a former UN Investigator in Bosnia currently researching terrorist financing at Oxford University, explain.**

**T**housands of nervous customers lined the streets of Macau in September 2005 to withdraw their funds from a bank tainted by the US authorities as a ‘primary money laundering concern’. The bank’s clients included parties that distributed counterfeit currency and smuggled counterfeit tobacco products. The run on the deposits totaled more HK\$300 million (nearly 10% of their capital) and underscored the consequences of being linked with a money laundering scam.

In 2003, the Financial Action Task Force (FATF) listed “counterfeiting and piracy of products” in its revised forty principles for money laundering as one of the 20 minimum predicate crimes for money laundering. This category covers a range of businesses impacted by intellectual property rights (IPR) theft from tobacco, apparel, pharmaceuticals, and software industries and presents a new dimension of AML compliance for financial institutions (FIs).

## A difficult war

We asked the FATF for its views on money laundering the proceeds of IPR theft. Professor Kader Asmal, the task force’s president says: “Those who break the law do not simply use

ordinary banks to deposit their ill-gotten gains. They launder their money, depriving countries and IPR holders of their legitimate benefits. The FATF 40 + 9 Recommendations impose obligations on all of us to stop such behaviour.”

Yet, IPR theft is still widely perceived as a victimless crime. In some countries on the US’s Special 301

Watch List (and others not on this list), members of the judiciary/law enforcement agencies believe IPR theft is unworthy of prosecution or sentencing, and adequate resources are not invested in investigations. However, the reach of AML regulations in many jurisdictions now covers IPR theft and this permissive culture will expose FIs to new risks in markets where there is a mismatch.

Each year IPR theft erodes the market for genuine goods and services. Local companies, MNCs and governments lose billions of

*“The FATF 40 + 9 Recommendations impose obligations on all of us to stop such behaviour.”*

dollars and innovation suffers. There is a cultural loss from the impact of piracy on the viability of the entertainment and arts industry. Serious health and safety risks are posed by counterfeit pharmaceuticals, auto parts and aviation parts.

Historically, IPR theft has been treated as a commercial issue for trade negotiators to haggle over, albeit it increasingly poses a security threat to countries:

- Much of the production and distribution is under the control of organised crime groups with profits rivalling, and in some cases surpassing, that of narcotics.
- The penalties are low when compared to drug trafficking and the high-profit, low-risk appeal of IPR theft attracts terrorist organisations.
- The perception of IPR theft as a victimless crime makes it susceptible to easier influence from corrupt public figures who interfere with the enforcement process.

#### *Size and scale*

- According to an Interpol report, the global narcotic trade, estimated at more than US\$322bn annually, has now been surpassed by the combined global piracy and counterfeit trade, which clears over US\$650bn.<sup>1</sup>
- Nearly 7% of the goods in the global marketplace are counterfeit.
- In China, Indonesia and Pakistan alone, more than 90% of the music and movies sold are pirated.

Counterfeiting is very diverse ranging from backstreet sweatshops to full-scale factories. Counterfeiters steal company secrets with the

help of corrupt employees or licensed suppliers and manufacturers who over-run production lines and sell the extra goods on the sly.

Distribution networks can be as simple as a stall in the street, or a shop on the other side of the world. The internet has helped with details on which goods to copy, and links to consumers and suppliers with ease and relative anonymity. The complex distribution network required by the larger counterfeiters has attracted organised crime.<sup>2</sup>

#### *Your war*

Six out of thirteen major Asian markets have already amended their anti-money laundering (AML) laws to include IPR theft. Some of the other countries are on their way to do this and others cover IPR theft under separate laws, albeit with different scopes and enforcement capacities.

Hong Kong, which amended its AML law in 2000, has successfully prosecuted several high-profile optical piracy cases with money laundering charges. In August 2004, Hong Kong Customs and Excise (HK C&E) neutralised a money laundering scheme that turned over HK\$4m in an 18-month period from the proceeds of pirated films.

*The combined global piracy and counterfeit trade clears more than US\$650bn annually, more than the global narcotic trade of US\$322bn p.a.*

Banks have a responsibility under AML laws to monitor for suspicious activity. By

<sup>1</sup> Zafar, Ziad. "The Big Steal" *Newline (India)* 11 July 2005

<sup>2</sup> *Economist* "Imitating property is theft", 15 May 2003

understanding the size, scale and financial needs of the counterfeiting and piracy industry, banks would be better placed to fulfil their statutory responsibilities. Using effective KYC check databases is a key aspect of this monitoring role. Suspicious transaction reports are an important input in investigations.

### Industry case study – Optical disc piracy

Optical disc piracy (ODP) is one of the newer forms of IPR theft that in recent years has flooded Asian and worldwide markets. The trade has become so lucrative, that the mark-up on a pirated DVD (1,150%) outpaces the differential profits of both heroin (360%) and cocaine (1,000%)<sup>3</sup>. Fortunately, Asian governments have woken up to this and have taken action; in 2004, 74% of worldwide DVD seizures were executed in Asia.<sup>4</sup>

#### Organised crime

Commonplace DVD/VCD pirate retail outlets are only the tip of the iceberg and larger piracy enterprises are similar to the Fortune 500 companies they steal from. These syndicates are also best placed to endure the costs of seizure and confiscation, and finding new ways to evade customs and policing authorities.

Raids in Hong Kong have picked up triad members implicated in local and export piracy operations that now contribute a major source of their income. The Chinatowns of London and New York are popular overseas destinations for these goods.<sup>5</sup> Elsewhere, ODP has become a key source of funding for the Malay and Taiwanese Triads, the Yakuza, La Costa Nostra, and the Red Mafiya.

<sup>3</sup> Estimates from *UK National Criminal Intelligence SU/Drug Project Report 2004*.

<sup>4</sup> Motion Picture Association Statistic Digest 2005.

<sup>5</sup> Seper, Jerry. "39 indicted in racketeering conspiracy" *Washington Times* (10 September 2005).

#### Terrorism

Terrorist groups find trading in counterfeit or pirated goods as an easy way to finance their operations with low-entry costs and high-profit margins. The triple border frontier (Paraguay, Argentina, Brazil) is overrun by the sale of such goods and is a black hole for financing of Islamist terrorist groups linked in to the counterfeit and piracy industries in Pakistan and Turkey. Intelligence agencies in

### Anti-ODP operations (DVDs/VCDs) Asia-Pacific 2004

- 25,000 investigations initiated
- 12,000 raids
- 49 million illegal optical discs seized
- 8,000 legal action initiated
- US\$896m lost in potential revenue

*Source: MPAA Statistical Digest, 2004*

Thailand and the Philippines have also been investigating terrorist groups involved in the pirated and counterfeit good smuggling from Malaysia and Indonesia.<sup>6</sup>

#### Money laundering exposure

The money laundering risks from ODP are derived from the business practices of the piracy syndicates. There are three broad groupings of piracy operations (large, medium, small), with each enterprise engaging financial services with different needs. The large and medium piracy enterprises have transnational businesses covering both manufacturing and distribution; they frequently use e-commerce to facilitate transactions. Counterfeiters and pirates are

<sup>6</sup> BBC Monitoring Asia Pacific. "Philippine daily views statement on MILF Jemaah Islamiyah links" *The Philippine Star* (29 September 2004).

also difficult to spot as many of their businesses are quasi-legitimate and produce both genuine and counterfeit goods.

#### *Financial services needed*

The financial services used by piracy enterprises include:

- Letters of credit for container shipments
- Insurance on shipping, building/facilities and manufacturing equipment
- Loans for purchasing new equipment, supplies etc
- Corporate accounts to execute payroll and manage overhead costs
- Money transfer facilities to remit funds to beneficiaries in several countries.

#### *Large enterprises (US\$3m+ p.a.)*

Large piracy enterprises are sophisticated/organised and undertake many placement and layering strategies to launder their proceeds, including the use of numerous front businesses and the full suite of financial services exposing FIs to serious reputation and financial risks.

Convicted pirates can default on loans when served with asset forfeiture and confiscation orders. Insurance services are also ripe for fraudulent claims to offset losses from enforcement seizures elsewhere in the world.

#### *Medium enterprises (US\$1-3m+ p.a.)*

Medium piracy enterprises will share many of the same transnational money laundering strategies employed by their larger counterparts, but on a smaller scale as they do not have as many front businesses to facilitate placement transactions. The risk of delinquency and fraud on financial products is greater as they cannot afford to wait out periods of heightened IPR enforcement.

#### *Small enterprises (< US\$1m p.a.)*

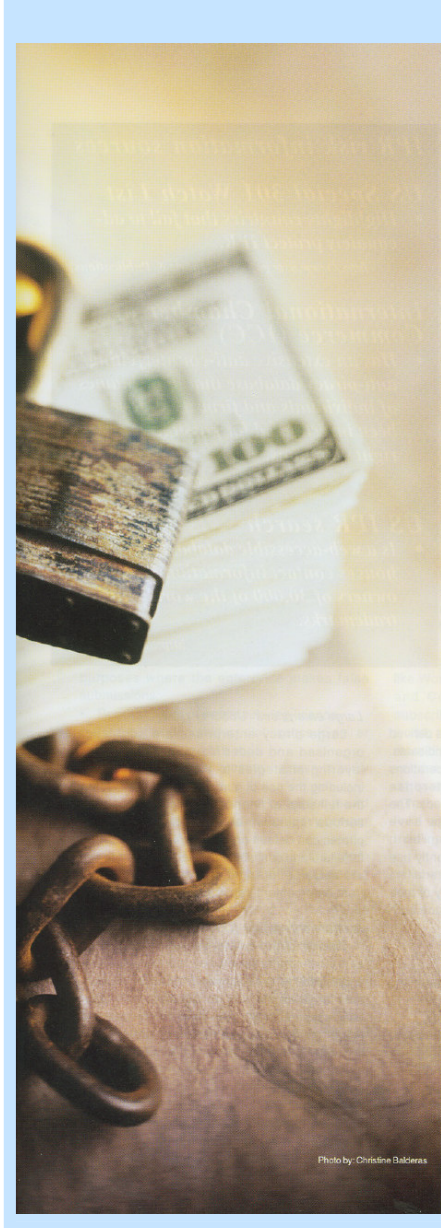
Small piracy enterprises reflect the risks associated with typical cash-intensive businesses and cash deposits/money transfers are the key facilities to watch. As of now, these enterprises use the banking system to transfer monies.

#### **Prevention strategy: AML risk models**

It is important for FIs to take a holistic risk-based approach in designing their AML programme. Specifically, in order to fight ODP, the key is for banks to build a new layer of ODP-linked intelligence into their existing AML risk models.

#### Geography and country risk

The US has a Special 301 Watch List. Special 301 is a law designed to monitor, and in extreme cases sanction, countries that fail to adequately protect intellectual property. Names on the *priority watch list* in Asia include China, India, Indonesia, Pakistan,



Philippines; the *watch list* includes Korea, Malaysia, Taiwan, Thailand and Vietnam.

Specific to ODP the list of countries leading the export of pirated goods in Asia include Malaysia, Pakistan, China, Indonesia, and the Philippines. The two trans-shipment hubs of Asia, Singapore and Hong Kong, may be exploited for shipping such pirated goods and customs have to be vigilant.

### Business and entity risk

The following steps may be useful for KYC purposes where the enterprise makes false submissions:

- Request proof of manufacturing licence.
- Request written evidence of licence to sell or reproduce copyright goods.
- Contact local IPR enforcement agency to verify status of licence.
- Public record search for prior conviction record of the associated individuals, company or other regulatory actions.
- Check for listing on blacklists from international enforcement agencies, including Interpol.
- Check with copyright holders (via the Motion Picture Association and the International Federation of the Phonographic Industry).

However, if the business is a semi-legitimate one and records their legitimate business while applying to the bank, traditional AML controls would help to spot suspicious activity like payments not in line with the banks understanding of the client's operations (geographies, parties, amounts), cash deposits for a business that declares its markets as being primarily overseas etc.

### Product and transaction risk

Offshore banking and private banking services are typical exploits of large piracy enterprises through their nominees including lawyers and company incorporation agents. Other services used are loans, cash, monetary instruments issuance/deposits, and critically remittances including the usage of unrelated third parties to facilitate transactions. Fully secured loans may also have their deposits forfeited under asset forfeiture laws leading to direct losses for banks.

### *IPR risk information sources*

#### *US Special 301 Watch List*

- **Highlights countries that fail to adequately protect IPR.**

*<http://www.ustr.gov>*  
(See Reports & Publications)

#### *International Chamber of Commerce (ICC)*

- **Has an extensive anti-counterfeiting/anti-piracy database that holds names of individuals and firms that have been investigated for possible copyright violations.**

*<http://www.icc-ccs.org/>*

#### *US IPR search*

- **Is a web-accessible database that houses contact information for the owners of 30,000 of the world's largest trademarks.**

*<http://iprs.cbp.gov/>*

### **Towards a new partnership**

IPR theft can no longer be regarded as a victimless theft and banks must play out their AML/CFT monitoring role. William O.T.

Chow, assistant commissioner (intelligence and investigation), HK C&E highlights: "Having a strong working relationship with the financial community is absolutely critical to effective IPR enforcement."

Mike Ellis, SVP and regional director, Asia Pacific for the Motion Picture Association (MPA) underscored the theme of cooperation. "Through close cooperation and good relations with law enforcement agencies and governments, the MPA has generated tens of thousands of criminal investigations around the region over the past five years," he says.

Critically, leading online KYC database vendors like World-Check, IntegraScreen Online, Factiva, and Complinet whose KYC products are subscribed to by thousands of FIs around the world, must focus on the issue of IPR theft in a more direct and proactive manner. KYC database vendors have to work with leading industry organisations concerned with IPR theft to make sure their databases highlight key players and their links so the battle can be fought directly on the frontlines where it hurts the criminals the most.

Disclaimer: the opinions in this article are the authors own and do not represent the organisations in which they work and are/were associated with.