

**Making your case to management:
Demonstrating the success of your programme,
Focus on financial crime and misconduct screening &
surveillance**

Peter R. Hazlewood
Managing Director
Group Compliance Services & Security
DBS Group Holdings Ltd

This Presentation

- Screening and surveillance stakeholders: who does what?
- Screening and surveillance activity streams: what are we looking for?
- Establishing the need for a screening and surveillance system and obtaining budget approval
- Obtaining benchmarking data
- Measuring effectiveness of implementation and operating model
- A topical Asian case study

Screening & Surveillance Stakeholders

- **The AML/Financial Crime Director (and part time salesman)** establishes the need for a system, obtains budget approval, is overall programme sponsor, agrees SLAs, approves the operating model and monitors effectiveness.
- **The Corporate Technology project team** designs the architecture, establishes source system feeds, formats source data, runs tests (such as data quality and system stability), moves the system into production then tunes and stabilizes the system.
- **The Business Analyst** designates which source systems are to be used, which lists are to be screened (and how often), sets policy on which products are monitored, the frequency and intensity of monitoring, designs the operating model and determines the outcome of a potentially suspicious transaction or watch list match.
- **Financial Crime Investigators/Analysts** review system alerts and either close/reject or escalate into 'case' status, then investigates and either closes or escalates a potential STR and manages customer and cross business/product impact.
- **The Surveillance Manager** trains and develops analysts, reviews and approves potential STRs, issues management reports, further tunes the system and reacts to changes in crime typology by writing new rules or changing parameters.
- **Shareholders and Customers** pay for the system and surveillance staff. In exchange they demand maximum operational effectiveness and optimal cost efficiency.

Screening & Surveillance Activity Streams

- Screening: Real time watch list filtering
 - Regulatory or supra-national body caution and sanction lists
- Screening: Near real time or batch watch list filtering
 - STR/SAR names/entities, prior investigations, credit lists (predictive analytics), subpoenas/production orders, PEP, media sweep data etc
- Surveillance: Near real time or batch external fraud
 - Card skimming, Ponzi schemes, phishing, account takeover, boiler rooms, cheque frauds, 419 etc
- Surveillance: Batch insider fraud & misconduct
 - Theft, adjusting personal or associated person's limits, deletion of charges, insider dealing, expense fraud, use of customer data, churning, payments from customers, payments between employees etc
- Surveillance: Batch money laundering
 - Structuring, unlicensed remittance agents, cash pooling agents, loan-sharking, repeated early product redemption, third party payments, TC strings, card credit balances etc
- Surveillance: Batch policy breach
 - Unauthorised access to customer or trade data, dealing with personally associated accounts, unauthorised securities trading, switching etc

I would like 30 Million dollars please....

What your CEO will ask.....

- Why do we have to do this?
- What is the specific P&L impact?
- What are our competitors doing?
- Why is this a priority over other strategic initiatives?
- Why can't we just install a single system to address that exam point?
- Can we build a cheaper tactical system in-house?
- How will I know it works?
- What are the cost benefits?
- How do I know you aren't going to come back in 3 years and ask for a new system to replace this one?
- What is the ongoing cost of ownership?
- Why are you asking me for a Rolls Royce when a Nissan will do?
- If I approve this will we have nothing at all to worry about?

And every subsequent year at budget approval....

Your CEO, CFO, CRO will ask.....

- Why does this continue to be a priority over other strategic initiatives?
- What is the P&L impact next year?
- What cost benefits have you delivered?
- What are the operational efficiencies that have been delivered?
- How can we tell that it is working effectively?
- Why didn't it spot *that* case in....

Making Your Case

- **You are selling an improvement in symptoms, not a panacea**
- **Benefits of a single integrated financial crime surveillance system (or at least a geographically integrated AML/watch list surveillance and screening system)**
 - Cleaner and lower cost architecture (hardware leases, system support charges)
 - Lower ongoing licence costs
 - Lower data storage costs
- **Benchmarking**
 - What are best in class banks doing? Surveys can be instructive. (the '5 year view)
 - What are your peer banks doing and how do you benchmark against them? (do not forget to agree in advance who your peer banks are)
 - What do the supra national bodies suggest? (example... BIS)
- **Enhanced operational effectiveness**
 - Less breaches and headlines!
 - Improvement in effectiveness ratio
 - Analysts can recognise suspicious activity beyond simple cash structuring or underground MSBs
 - Fraud loss reduction
- **Integrated operating model**
 - Efficient: Less staff required for leave/shift cover and in a hubbed model, they can do more
 - Integrated model allows for job enrichment and reduces costly attrition
- **Legacy system redundancy**
 - Inadequacy of legacy system
 - Age/ability to react to new financial crime typologies (new rules etc)

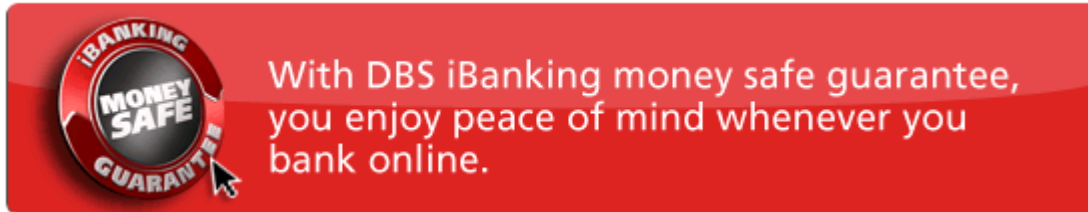
Making Your Case

- **Financial ‘Air Traffic Control’**

- Spoken to Finance and sequenced the spend to fit with other strategic initiatives
- Present the case showing P&L impact (OpEx and CapEx) over the course of programme rather than one off cost and include ongoing cost of ownership
- Pre agreed cost allocation methodology with business line controllers

- **Regul**

- St
- N
- O

A red rectangular graphic with a circular seal on the left. The seal has 'iBANKING' at the top, 'MONEY SAFE' in the center, and 'GUARANTEE' at the bottom. To the right of the seal, the text reads: 'With DBS iBanking money safe guarantee, you enjoy peace of mind whenever you bank online.'

- **Focus on pockets of risk**

- Implement in higher risk product group/jurisdictions first

- **Business benefits**

- Customised reports can be produced for client groups
- Enhances the customer experience (limits, guarantees, phone number registration, repeat use of one time password “OTP” token etc) which sets your institution apart from competitors

- *“some banks need for speedy (system) implementation has clashed with the goal of developing an optimal end product....”*

ABA Bank Compliance Dec 2007

Monitoring Effectiveness

- How can you monitor the effectiveness of your surveillance programme?
- Overview of dashboards
 - **Example used: Real time watch list filtering**
 - Batch watch list filtering
 - Batch money laundering
 - Near real time and batch external fraud
 - Batch insider fraud and policy breach

Optimizing Implementation Effectiveness

- Look at every stakeholder and every activity stream
- Map all activity streams and decide exactly what needs to be done in order to optimize surveillance effectiveness. Think in terms of:
 - The scope of implementation (countries, products, activity streams)
 - The process of building a system, testing it, moving it to production, tuning and stabilization.
 - The desired architecture; for example: Do you wish to take feeds from individual source systems or via a data warehouse?
 - The source data platforms that are required to feed the screening and surveillance system
 - The critical data fields that must travel to the rules engine from the source systems in order for the system to do its job
 - Opposite account key
 - Staff ac identifier
 - Cheque sequence
 - Related ac
 - Dormant, hold-mail, potential vulnerable ac tags
 - Critical external ac series
 - Industry codes
 - The lists that require screening against
 - The optimal (and interim) operating model
 - How to measure effectiveness post implementation

Developing Dashboards

Example: Real Time Watch List Filtering

| | | | | | | | | | | | | | | |
|---|-------------------------|---|----|----|------------------|--------------------------------|---|--------------|---|---|---------------------------|---------------------------|---|--------------------------------|
| Real Time Watch List Filtering (Payments & Trade) | Source Systems | Payment/trade platform (100%) | | | | | | | | | | | | |
| | Technology | Testing (25%) | | | Production (25%) | | | Tuning (25%) | | | Stability (25%) | | | |
| | List Data | Global regulatory lists, English language lists (75%) | | | | | | | | | Local language lists(25%) | | | |
| | Operating Model | SLAs in place with T&O (reporting cutoffs, defects etc) (20%) | | | | Staff training and exams (20%) | | | Advisory process loop & committee reporting (20%) | | | List upload Process (20%) | | Staff workload benchmark (20%) |
| | Effectiveness | J | F | M | A | M | J | J | A | S | O | N | D | |
| | Block submissions | 57 | 52 | 34 | | | | | | | | | | |
| | Genuine blocks | 32 | 30 | 17 | | | | | | | | | | |
| | Missed cases (breaches) | 2 | 0 | 0 | | | | | | | | | | |

- (a) Every box has an overall owner and underlying task list with issue owners assigned and target completion dates
- (b) Each box is weighted according to priority and measurable objectives are set to upgrade/downgrade status
- (c) Individual and team performance management flows from this process (i.e. KPIs)

Example of measure of effectiveness for RTWLF

- Zero breaches
- Improving trend between number of block submissions and genuine blocks
- Improving trend, number of genuine blocks

Examples of issues potentially impacting effectiveness:

- Stability: Zero outstanding severity level four (“SL4”) tickets with aging > 6 weeks and zero outstanding SL1,2 and 3 tickets with aging > 2 weeks and minimum 99.5% application availability
- Training: Training programme in place for all surveillance analysts covering confirmation of a block, lookup and interpretation of core sanctions, list maintenance procedures, operation of surveillance system, SLAs. All ANs CAMS certified. All passed internal exams >80%
- Staffing: Alert (or case) per AN per month <25% higher than industry benchmark >3 months
- Tuning: Not more than 2% of messages flagged for further screening (insufficient lower risk tokens added)

Obtaining benchmarking data

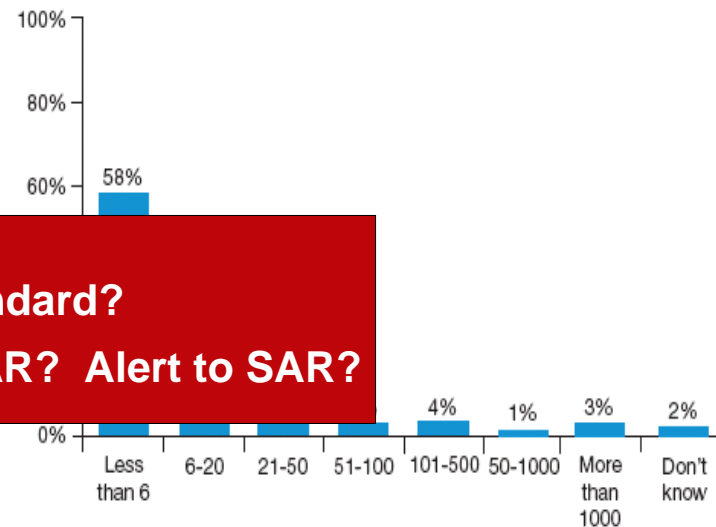
- Celent
 - System functionality
 - Vendor reviews
 - Industry trends
 - Emerging technology
- PwC AML Survey, Op Risk & Compliance Survey, KPMG Survey
 - Monitoring methods used
 - Industry and geographic trends
 - False positive ratio
 - Trends in compliance spend
 - SAR filing trends
- Regulators & supra national bodies
 - Required system scope and coverage
 - SAR trends
 - False positive ratio
 - Cross industry thematic inspection and benchmarking reports (lists being screened)
- Surveillance system and data vendors
 - False positive ratio
 - Industry trends
 - Emerging technology
 - Tuning and stability benchmarks
- Formal and Informal industry groups and associations
 - False positive ratio
 - Case volumes, staffing levels and workloads
 - Operating model
 - Industry trends
 - Budget spend

Example: What is the false positive benchmark?

Figure 6: The rate of false positives experienced for those respondents that indicated a rate in excess of 30%.



Figure 5: The number of Suspicious Transaction Reports / Suspicious Activity Reports made by each organisation per year.



**What is the standard?
Alert to Case? Case to SAR? Alert to SAR?**

“over four fifths (84%) of respondents stated that their automated systems generated at least 30% false positives. Of more concern was that 96% of these specific respondents indicated that their false positives rate was actually equal to or higher than 90%. Specifically, five respondents told us that they had a 100% false positive rate indicating that they get no value at all from their automated monitoring system”

Performance measures worth considering:

- **Fraud investigations developed as % of logical entity alerts**
- **Potential fraud loss prevented (as at next statement date)**
- **Number of positive name matches**
- **Positive matches as a % of alerts**
- **False negatives identified**
- **Number of breaches**
- **Number of SARs filed as % of logical entity alerts**
- **Accounts closed**

Opportunity for ACAMS?

- Conduct and publish thematic industry surveys
 - Overall model used
 - Caseloads
 - System effectiveness
 - Areas of spend
- Suggest industry wide measurement standards
 - Av. caseload per Analyst per month
 - Alerts per Analyst per month
 - System effectiveness ratio ? Alerts ÷ SAR ? Cases ÷ SAR ?
 - Measured as a percentage of logical entity or absolute number of alerts?
- Benchmark internal training programmes

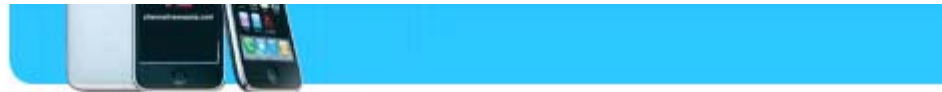
Case Study Loan Sharking

Disclaimer: The information contained in this document is intended only for use during the presentation and should not be disseminated or distributed to parties outside the presentation. DBS Bank accepts no liability whatsoever with respect to the use of this document or its contents.



Loan Sharking

- ...a person or body that offers unsecured loans at high interest rates to individuals, often backed by blackmail or threats of violence.
- In Singapore/ Malaysia: **Ah Long** (derived from the Cantonese phrase '大耳窿').
 - Lend money to people who are unable to obtain loans from banks or other legal sources (e.g., those with no income),
 - Mostly targeting habitual gamblers
 - Charge a very high interest rate (about 40% per month/fortnight which equals 1422%/33087% per annum due to the constantly compounding interest)
 - Frequently threaten violence (and administer it) towards those who fail to pay in time
 - Use of “O\$P\$” as intimidation



Sharp r

Tags: [loansharks](#)

AFP

SINGAPORE - economic cri said Monday

There were 1 from 11,800 department.

Illegal money pressure deb

"We expect see how it w

HOME

ASIA PACIFIC

SINGAPORE

WORLD

BUSINESS

SPORT

TECHNOLOGY

ENTERTAINMENT

HEALTH

SPECIAL REPORTS

BLOGS

YOURnews

Day News Archive
M | T | W | T | F | S | S

Search **GO**

- iPhone App
- Android App
- Mobile News



[Video](#) [Finance](#) [Lifestyle](#) [Travel](#) [Weather](#) [Discussion](#)

[Home >](#)

SINGAPORE NEWS

20 arrested in connection with loan-sharking activities

Posted: 08 January 2010 1611 hrs

SINGAPORE: Police have nabbed 20 people, mostly men, for assisting in the business of unlicensed moneylending.

They were arrested in raids conducted in Ang Mo Kio, Bedok, Hougang and Robinson Road.

Preliminary investigations showed that the 20 suspects had opened bank accounts and given away their Automated Teller Machine (ATM) cards and Personal Identification Number (PIN) to loan-sharking syndicates for loan-sharking activities.

Moreover, 17 of them are believed to be debtors themselves.

All the bank accounts have been seized and investigations are in progress.

Under the Moneylenders Act, when a bank account or an ATM card of any person is proven to have been used to facilitate the business of an unlicensed moneylender, that person is presumed - until the contrary is proven - to have assisted in the business.

First-time offenders found guilty of such an offence may be fined up to S\$200,000 or jailed a maximum of two years, or both.

Repeat offenders face a fine of up to S\$200,000 and a mandatory jail term of up to five years.

n July 3- and

all 9.5 loan rs end

ss / a hus

ince on g bully-

care

g fires

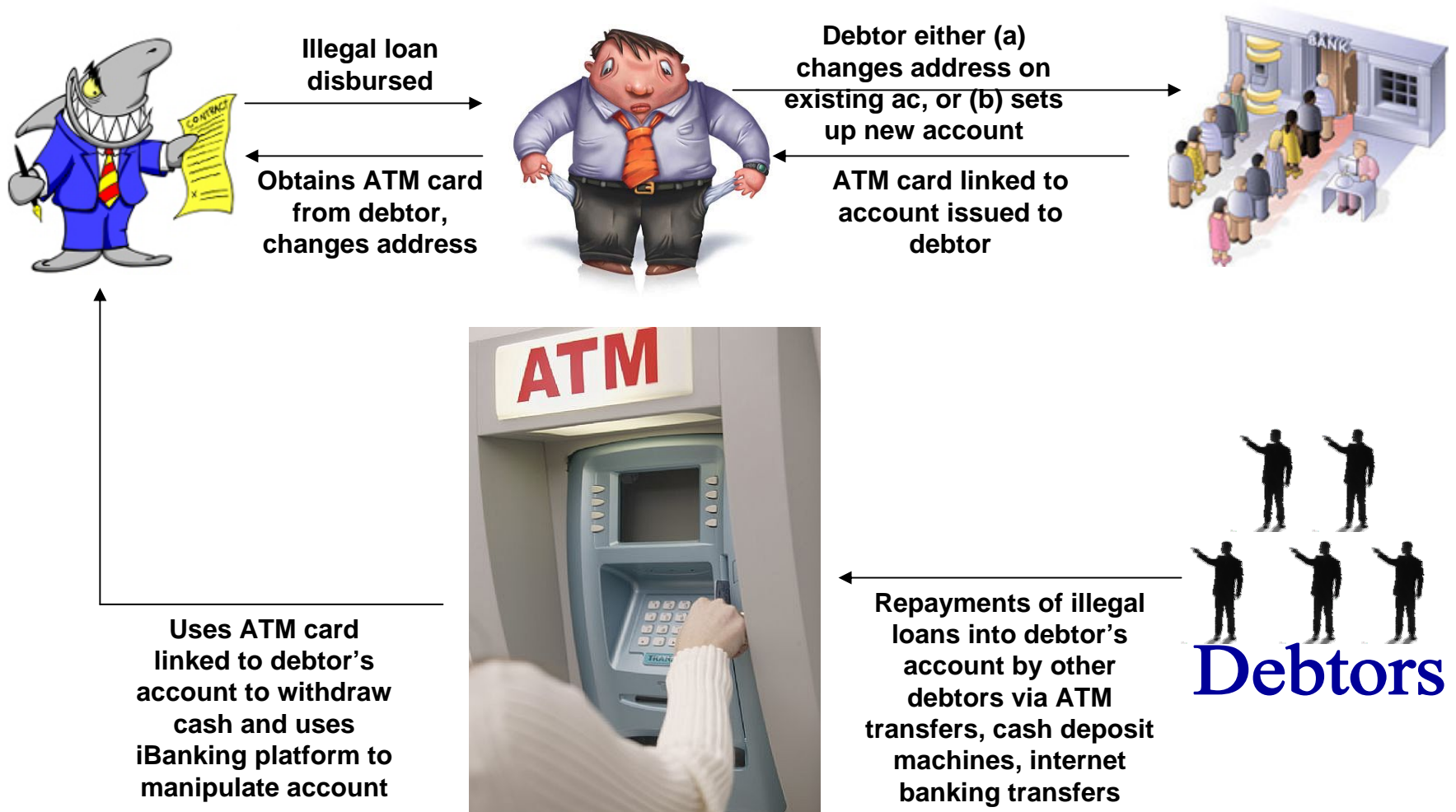
her

bombs

Their Calling Card.....



Loan Sharking



69 SARs filed 2008/2009.

Sept to Dec 2009, 195 production orders

- Change of address
 - Accounts taken over from locals or foreign workers
- Pattern of matched debits/credits
- Balance returning to zero after matched transactions completed
- Sudden change in transaction volume
- Higher than average transaction volume (10-20 per account per day)
- Production order intelligence process linked to surveillance
 - i.e. case management system used as a feed for batch watch list screening
- Link analysis to identify broader syndicate (using internet or ATM transfer)

- *“Financial institutions are maintaining the attitude that risk management and compliance is merely a cost of doing business. Instead financial institutions should approach risk management and compliance as an opportunity to build customer confidence, increase revenues and decrease IT spending.”... **AMEinfo.com, Feb 2007***