# Testing AML Systems Through Anonymous Customer Interaction With Financial Institutions Frontline Staff

## 'The Mystery Shopper Process'

## Why Testing of AML/CTF Systems is Essential

### Recommendation 1 and Immediate Outcome 1

"Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, […] and apply resources, aimed at ensuring the risks are mitigated effectively."[1] "Effectiveness is the extent to which financial systems and economies mitigate the risks and threats of money laundering, and financing of terrorism and proliferation."[2]

The question is, 'how should a country identify money laundering and money laundering risk and how should they mitigate it?'

The method to-date has been to conduct National Risk Assessments which often draw on information on financial flows, levels of offending, numbers of prosecutions, numbers of STRs and the like. All of which are useful proxies for information on money laundering but do not necessarily provide a full picture. A potential flaw in these processes arises because such proxies potentially only provide information about risks that have, already been identified.

STRs may provide some information outside of typologies that are already known, however, as the results of previous Mystery Shopper programs have shown, staff of financial institutions who are tasked with submitting STRs often rely heavily on directions and information from regulators on identifying red flags. This situation has the potential to provide a self-perpetuating loop – regulators highlight ML methodologies that are already known, FI staff look for indicators of such offending as directed, they report STRs accordingly and the prosecutions that arise relate to already known methodologies. All while potentially overlooking significant money laundering going on unnoticed[3].

[1] FATF Recommendations 2012

[2] FATF Methodology for Assessing Compliance with FATF Recommendations and the Effectiveness of AML/CTF Systems (2013)

[3] The Australian Federal Police have an example of this. Bank staff, when questioned as to why they had never reported the people who came into branches with backpacks full of cash and made deposits into third-party accounts just under the reporting threshold responded that such behaviour had always gone on and therefore wasn't deemed (by them) to be suspicious.

A significant problem arises, as has been the case in some jurisdictions, when those tasked with submitting STRs are the same people conducting the laundering.

A National Risk Assessment perhaps should include information on say, the level of effectiveness of training of frontline financial institution staff, or, the willingness of financial institutions and DNFBPs to reject potentially profitable business involving illicit funds, or, the willingness of financial institutions to engage in and assist their customers to engage in money laundering. It perhaps also should include information on the effectiveness of border currency searching capacity, or the capacity and willingness of casinos to detect and report (or reject and report) suspicious activity.

In fact, ideally a National Risk Assessment perhaps should be informed by a range of statistics and information on all aspects of the AML/CTF system and how well they are functioning. From the effectiveness of financial institution staff in identifying and responding to suspicious activities to the ease or difficulty with which smurfing might be conducted to the ease or difficulty with which an anonymous company or structure might be able to gain access to a bank account.

A national AML system that is passive, that doesn't test the systems and processes for effectiveness , or actively seek to identify money laundering and terrorist financing and the methodologies through which they occur, may possibly only ever be partially effective .

One method for addressing these deficiencies is active testing of AML/CTF systems through a Mystery Shopper process.

## Other Recommendations Relevant to Mystery Shopper Testing

Two other Recommendations may be viewed as supporting AML/CTF systems testing, these are Recommendation 26 and 28. Recommendation 26 on Regulation and supervision of financial institutions requires countries to ensure that financial institutions are subject to **adequate regulation and supervision and are effectively implementing the FATF Recommendations**. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for **monitoring and ensuring compliance** with national AML/CFT requirements.

Similarly, Recommendation 28 on Regulation and Supervision of DNFBPs requires countries to ensure that competent authorities ensure that casinos are effectively supervised for compliance with AML/CFT requirements and that other DNFBPs are subject to **effective systems for monitoring and ensuring compliance** with AML/CFT requirements.

It is arguable that there may be no better means of 'monitoring and ensuring compliance' than through active testing.

## Mystery Shopper Methodology - from Other Situations

The concept of a 'mystery shopper' comes from the assessment of customer service in shops by a person, who is unknown to the shop staff being assessed. The Mystery Shopper visits the shop and purchases an item as a normal customer would. The Mystery Shopper then records the

good and bad points from their shopping experience and the data is used to make an assessment of the business or the staff.

Such methodology has been used to compare businesses in a town or region for business awards. Other uses of such a process is to enable management to gather information on customer experience, staff training, staff morale and the like in order to allow improvements to be made.

## Methods of Testing of Systems in Other Situations

In today's age of cyber-terrorism it would be highly unlikely for a national agency or large company to deploy an information and communication technology (ICT) system or software that had not been tested against hacking, exploitation or systems faults. Ironically, however, many countries and jurisdictions around the world currently have in place AML systems that have been developed and deployed and rely entirely on the assumption that they are fit for purpose and remain almost completely untested.

Like AML systems, ICT systems are vulnerable to harmful exploitation. Also like an ICT system, those doing the exploitation rarely announce their success. They attempt to operate in secret, cover their tracks and utilise vulnerabilities that are unknown to those who have set up the system.

For many years governments and system software providers have made (or engaged others) to make deliberate attempts to infiltrate and hack systems or software. Such testing provides vital data on weaknesses and allows for corrective action, or patches to be implemented.

The Mystery Shopper process is analogous to the attempted exploitation, circumvention or 'hacking', of a country's AML systems in order to provide intelligence on weaknesses and allow for corrective action to be implemented.

## Identifying Implicit Assumptions Contained in AML/CTF Systems.

Implicit in many jurisdiction's AML/CTF systems is the assumption that gatekeepers will be proactive in preventing offending by their customers.

Also implicit in the assumptions is the belief that law enforcement will be capable of dealing with the numbers of STRs reported and that prosecutions for money laundering and related AML/CTF offences will occur in sufficient volumes to provide a deterrent both to individual launderers, syndicates, gatekeepers, facilitators, financial institutions and DNFBPs.

Numerous Mutual Evaluation Reports have shown that for many, if not most, jurisdictions prosecutions for money laundering are low in comparison to the levels of predicate offending thereby providing little in the way of deterrent for launderers of all types.

Prosecutions, or punitive action, for other AML/CTF related offending such as failing to report STRs, failing to report threshold transaction reports etc are arguably also below levels likely to provide a deterrent in most jurisdictions.

Furthermore, the levels of STRs in many jurisdictions are at levels that overwhelm FIUs, regulators and law enforcement.

For AML/CTF systems predicated on financial institutions and DNFBPs being the gatekeepers identifying, reporting and preventing laundering, effectiveness unfortunately, relies on those gatekeepers being willing to not only identify and report ML and TF but also to be proactive in terminating otherwise profitable relationships.

Experience has shown that this is less likely to occur in jurisdictions where financial institutions and entities have little or no cause to fear detection or prosecution but even in jurisdictions such as the US, the level (and perhaps type) of punitive action does not appear to be stemming the tide of offending.

Proxy measures of effectiveness of AML/CTF systems such as the number of STRs reported compared to GDP, prosecutions, restraint actions etc, have the potential to be misleading in determining the effectiveness of a country's AML/CTF systems. This is because it is all but impossible to determine whether a large number of prosecutions or restraint action is because there is a lot of financially motivated crime or whether the authorities are particularly effective in detecting and prosecuting. Similarly, a high volume of STRs may indicate an effective reporting system or hide large numbers of repeat STRs about the same people[4] (indicating a disinclination on the part of institutions to cease business with criminals) or large volumes of defensive or 'junk' reporting.

A potential example of the difficulties facing regulators lies in the low level of prosecutions for failing to properly train staff to identify and respond to suspicious transactions and events. It may be that the difficulty arises from regulators trying to prove that financial institution staff had not been properly trained when an institution claims otherwise. Regulators have often been drawn to the existence of a training program (and less commonly, exam results from staff testing) however these alone do not prove that staff are adequately trained.

Recent years have provided numerous examples of financial institutions that were not only unable to identify or report ML but were willing to engage in, and actively court, business with criminals and those who wished to circumvent sanctions.

The difficulty for regulators is determining which institutions and entities are acting legally and appropriately and which are not. A Mystery Shopper program has the potential to identify those institutions and allow regulators to focus attention on them.

[4] A bank in Pacific country apparently reported a single individual over 100 times before deciding to terminate the relationship. The AML regulator in that country apparently never commented or advised – hardly a measure of an effective system.

## Reliance on private enterprise potentially inappropriate

A typical answer to a question such as 'Who is responsible for detecting money laundering in your country?' is ' banks or other financial institutions'. This reliance, where it occurs, possibly overlooks the fact that financial institutions are first and foremost profit driven and appear (at least in the some countries) to be factoring fines for AML deficiencies into the ordinary cost of doing business.

If, as appears may be the case, that some financial intuitions would rather pay a fine than go to the trouble and expense of implementing effective AML systems, the reliance on these institutions to detect ML and FT may be somewhat naïve.

A Mystery Shopper process has the potential to actively identify money laundering weaknesses and support targeted intelligence collection to identify money laundering or terrorist financing.

## What Mystery Shopper process does not test

The Mystery Shopper processes do not test 'risk'. In identifying specific instances of AML failings such as, a financial institution failing to report suspicious transactions or failing to conduct appropriate customer identification or actively assisting a customer to circumvent AML controls, the Mystery Shopper process allows for the collection of information or intelligence on AML systems weaknesses.

The information collected during the Mystery Shopper process may be able to be used to infer the risk of other sections of the AML system having similar failings, such as other financial institutions acting criminally, however such an inference may need to be supported by additional data.

The intention of the Mystery Shopper process is to allow identification of actual AML failings and to allow corrective action to be undertaken.

If for example it is identified that financial institution frontline staff were incapable of identifying and responding to money laundering or terrorist financing it may be determined that the AML weaknesses arose due to a lack of education, guidance or information. If however the staff were capable of identifying money laundering but were unwilling to respond in an appropriate way this may call for an entirely different response. Either way, the Mystery Shopper exercise has not measured the risk of money laundering, it is gathering data on actual events from which risk may or may not be inferred.

# Developing Mystery Shopper Tests

Testing of AML systems has the potential to be as simple or complex as required, however, there may be advantages in terms of resource requirements by commencing with areas already deemed to be high-risk.

Development of tests requires a working knowledge of the AML systems in place. For example, if the jurisdiction does not collect threshold cash transaction reports it would clearly be futile to conduct a test that 'smurfs' cash through financial institutions.

There is a good argument for (initially at least) developing tests based on three different criteria and three different stages:

The initial three criteria are:

1) The FATF Recommendations;
2) The local legislation;
3) Typologies and methodologies from other jurisdictions.

The three stages are:

1) Test for normal function of systems, processes, laws and guidelines;
2) Test for criminal activity in financial institutions and regulated entities;
3) Attempt to circumvent systems, processes, laws and guidelines

## Three Suggested Criteria for Developing Tests

### Criteria 1 – FATF Recommendations

1) The FATF Recommendations provide the base standard for AML/CTF effectiveness. Jurisdictions AML/CTF systems ideally should be capable of fulfilling the criteria that the Recommendations suggest. Demonstrating 'effectiveness' has been a significant challenge for many jurisdictions as most measures used or proposed to date have shortcomings. Naturally, not all recommendations lend themselves easily toward testing, however, those that more obviously do are listed below.

   10. CDD and Record Keeping
   14. MVTS
   15. New Technologies
   16. Wire Transfers
   20. Reporting of STRs
   22. DNFBP CDD
   23. DNFBP STRs
   24. Legal Persons
   25. Legal Arrangements
   32. Cash Couriers

### Criteria 2 – Local Legislation

Most countries and jurisdictions now have legislation in place criminalising money laundering however it would appear that far fewer have attempted to undertake controlled operations to 'launder' funds through their financial institutions. Such tests might yield significant intelligence on

the laundering methods that are likely to be successful (and therefore worthy perhaps of designation as 'high-risk' and subject to consideration for corrective action) and those that are unlikely to be successful

Local legislation that requires, for example, enhanced customer due diligence on foreign customers domiciled in tax haven jurisdictions might be worthy of being tested by attempting to open an account using a company domiciled in a tax haven jurisdiction.

Similarly, wherever feasible, all relevant local legislation may benefit from testing to ascertain the level of compliance by financial institutions and efficacy and therefore may be the basis of testing procedures .

### Criteria 3 – Typologies and Methodologies

There are a range of tied and tested methods of money laundering that keep being used – either in different jurisdictions, or, where a jurisdiction has failed to appropriately address weaknesses, in the same jurisdiction.

There is a good argument for formulating tests to ascertain whether common money laundering and terrorist financing methods are still capable of being used in your jurisdiction. There is also a good argument in support of formulating tests when new methodologies are discovered.

## Three Suggested Stages Of Testing

### Stage 1. Normal Functioning of Systems

Stage one testing might be viewed as the lowest level of testing. It is intended to test whether, for example, normal reporting obligations are in place and functioning appropriately.

Such tests might include conducting activities such as:

- Cash threshold transactions with financial institutions to test whether reporting is conducted in a manner consistent with laws and guidelines, inclusive of all relevant data and within timeframes;
- Border currency movements using declared cash to test border control procedures;
- Suspicious behaviour on a casino gaming floor to test reporting capacity;
- Approaches to financial institutions and engaging in suspicious behaviour (querying processes, depositing sticky, soiled or smelly cash, photographing/videoing security equipment, declining to conduct transactions or enter into a business relationship when asked for ID etc, etc) to test the ability of frontline staff to identify and respond appropriately to suspicious behaviour

- Conduct online or non-face-to-face business in a manner that is suspicious (conducting accumulation transactions into apparently un-linked accounts followed by international remittances)

## Stage 2. Testing for criminal activity in financial institutions and regulated entities

Testing for criminal activity is a more sophisticated level of testing and may require a greater level of covert operation ability as well as resources and planning.

Testing whether a lawyer, for example, will allow funds to be remitted through their trust account without obtaining appropriate customer information is more complicated than merely attending a branch of a bank with a notepad and tape recorder.

Testing for money laundering, terrorist financing or other relevant unlawful or criminal activity should be done in a manner that does not unduly endanger those conducting the testing and may best be conducted under formalised protocols and with relevant controlled operation protections/ procedures in place if there is the potential that laws may be contravened in the conduct of the tests.

Such tests might include conducting:

- Covert approaches (using an appropriate cover story) to lawyers/accountants/real estate agents, banks, insurance brokers and other known facilitators and recording responses to requests for assistance with money laundering .
- Covert approaches to high-value goods dealers attempting to use their business as a means of laundering
- Replication of previous money laundering methods using facilitators that have previously engaged in (or are alleged to have engaged in) money laundering activities.

## Stage 3. Attempt to circumvent systems, processes, laws and guidelines

Possibly the most complex form of testing involves attempts to circumvent AML/CTF controls, reporting, data collection etc.

Tests such as these, as with Stage 2 tests above may best be undertaken with appropriate formalised protocols and with relevant controlled operation protections/ procedures in place.

Attempts to circumvent controls may include activities along the lines of:

- attempting to open and operate bank accounts anonymously;
- conduct smurfing activities (without providing identification);
- conducting border currency movements using undeclared and secreted cash;
- value transfers into or out of the jurisdiction using credit/debit/stored value cards/ digital currency/etc;
- use of false/fake documentation to open an account, form a company or make a one-off transaction;

- establishing a relationship and/or conducting transactions through trust accounts of law/accounting/real estate firms or casino accounts without providing appropriate identification or using false ID;
- Attempting high-value goods purchases in circumvention of the local law (in cash/without appropriate ID etc)
- Attempting other money laundering and terrorist financing methods to gather intelligence and provide information relevant to addressing weaknesses.

## Developing Tests So That Results Can be Easily Recorded, Compared and Used

There may be advantages to developing tests that allow for distinct positive or negative outcomes rather than qualitative assessments which can be argued (and present difficulties in re-testing)

For example it may be easier to record and assess whether financial institution staff did or did not submit an STR following a suspicious approach or transaction by the Mystery Shopper than it would be for the Mystery Shopper to assess the level of the staff member's understanding of their legal obligations from the interaction.

Similarly, a transaction under the threshold into a third party account either succeeds or is prevented; a stored value card is loaded with funds and used in Afghanistan without being reported or it isn't; a company is created in a fictitious name and used to open and operate a bank account, or it is prevented; A DNFBP conducts appropriate CDD on a Mystery Shopper or they don't.

One use of the Mystery Shopper testing may be to capture evidence for punitive action against a financial institution or group of institutions in order to force or encourage compliance. If this is envisaged then the testing procedure including the format and the means of recording must be done in a manner that is acceptable to the court, tribunal or entity to which the evidence will be referred.

Often this will mean that the evidence must be recorded in a manner that does not breach laws on covert evidence gathering and the questions must be formulated in a manner that does not breach agent provocateur guidelines or laws.

## Testing and Recording Results

In order to be capable of being used for statistical purposes, reports and in the development and assessment of corrective action, the results must of tests must be recorded in a manner that is capable of ensuring validity and accuracy.

Where the tests involve face-to-face interactions there may be benefit to developing a script and recording (either through writing or electronic means), the questions and answers. Follow up meetings with financial institutions have been shown to benefit from accurate records of which staff member was spoken to and when as well as the answers that were given.

## Examples of Tests

## Testing the training of financial institution staff

Many jurisdictions rely heavily on financial institution staff and automated systems to identify high-risk activity and report it appropriately. There is considerable evidence that this reliance is naïve. Frontline financial institution staff, to whom the bulk of this responsibility falls are often lowly paid, experience high levels of turnover and are not always well trained.

- Attend branches or offices of financial institutions/DNFBPs/TCSPs and advise that you wish to move money from one tax haven to another (or, move large amounts of money internationally without drawing suspicion in order to pay a politician). Ask questions of the staff about their reporting processes. Ensure that the activity is suspicious by stating that the funds that are being handled or the process described does not make economic sense. Ask whether it is possible to structure or conduct transactions in such a way as to ensure that no report is sent to the government.

### Testing the willingness of financial institutions to engage in money laundering

Considerable evidence now exists that banks as well as lawyers, accountants, TCSPs, gambling and gaming providers etc are often all too willing to assist customers to money launder, break sanctions and, to a much lesser extent, fund terrorism.

It might be reasonable to approach financial institutions (particularly those that haven't been tested) with a level of professional scepticism about their potential willingness to turn away profitable business that involves handling the proceeds of crime.

- As with the test above attend branches or offices of financial institutions/DNFBPs/TCSPs and advise that you wish to move money in a way that does not make economic sense. Finish up by asking whether it might be possible to pay extra for greater assistance in hiding the beneficial owners or for no reporting to be sent to the government.

### Testing the willingness of financial institutions to turn away profitable business from criminal sources

- Attempt to open a bank account, purchase a company or purchase high-value goods in such a way as to leave the financial institution, DNFBP or TCSP in no doubt as to the fact that the funds you are to use can not be from a legitimate source. For example, state that you are currently unemployed, use a fake name, provide no source of income declare that you have been recently released from prison etc.

### Testing threshold transaction reporting by financial institutions

The timely reporting of cash transactions and international funds transfers above a certain threshold is a key plank of many AML systems. Unreported transactions, whether due to lax systems within financial institutions or due to financial institutions accepting bribes or being complicit in the laundering process have the potential to severely weaken the AML system of a country.

#### *Threshold Transaction Reporting Tests*

- Attend branches or offices of financial institutions and deposit/ place physical cash into the financial system in an amount above the threshold and test to ensure that the reporting of the amount, date, details of sender and receiver are reported accurately and in a timely fashion.

#### *Suspicious Transaction Reporting Tests/tests of the willingness of a financial institution to assist customers or clients to launder*

Suspicious transaction reporting is, for many jurisdictions, the primary means of detecting money laundering and terrorist financing.

- Attend branches or offices of financial institutions/DNFBPs/TCSPs and conduct a transaction or multiple transactions into third party accounts that are just below the reporting threshold
- Make multiple transactions just under the threshold limit from various branches into a single account to ensure that financial institutions are capable and willing to report such activity.
- Make deposits of unusual banknotes (wet, smelly, oily, large volumes of small denominations etc) in a manner that should draw suspicion.
- Make multiple deposits into the same account in a single day that are each just under the threshold
- For TF, make deposits into a third party account and advise the staff that it is to be transferred to a high-TF risk jurisdiction or make multiple small transfers to an account in Afghanistan, Iraq, Syria or another high TF jurisdiction

### Testing CDD around company and trust and legal structure formation or purchase

The appropriate identification of the beneficial owners of a company, trust or other legal structure is a key requirement of most AML systems. Testing whether trust and company service providers are willing to sell products without appropriate due diligence may provide regulators with data on a key weakness.

Testing this might be as simple as attending offices of TCSPs and attempting to purchase products without providing appropriate identification.

Some jurisdictions allow the formation/purchase of companies online. Testing whether this can be done without providing appropriate identification may similarly provide vital data on AML weaknesses.

While it is not suggested that jurisdictions attempt to test the systems in other jurisdictions there may be some benefit in knowing what weaknesses exist in neighbouring jurisdictions or jurisdictions that are known recipients of foreign proceeds.

### *Tests that might be considered - Trusts and Companies*

- Attempt to create a company online without providing appropriate ID (either false identification documents or fictitious details)

- Attempt to purchase a company, trust or other legal structure from a provider without providing appropriate ID (either false identification documents or fictitious details)
- If successful in obtaining such a legal entity attempt to open and operate a bank account using the entity.

## Follow-up Meetings

Depending on the type of testing and the results there may be benefit to meeting with the financial institution following the Mystery Shopper visit/approach.

Some jurisdictions have found that financial institutions will claim that there staff are well trained and that their systems are fully functional until provided with the evidence that paints a different picture.

A meeting with the institution may provide the basis for an agreement on the appropriate corrective action. If however the corrective action is to be the prosecution of an institution the follow-up meeting, if it occurs, may need to be part of a formalised legal process.

## Analysis of Results

The effectiveness of AML/CTF systems involves a significant degree of qualitative assessment. For example, the determination as to whether an STR is a good quality report pertaining to a genuine concern that the customer was engaging in unlawful activity or merely defensive reporting is a qualitative assessment.

The analysis of the results of the Mystery Shopper AML Systems testing will therefore involve a degree of qualitative assessment. There may be advantages however to designing tests that lean toward quantitative assessment and 'yes/no' assessments.

For example, it may be easier to record and assess whether financial institution staff did or did not submit an STR following a suspicious approach or transaction by the Mystery Shopper than it would be for the Mystery Shopper to assess the level of understanding of their legal obligations from the interaction.

## Reporting Results

It is possible that there may be a range of uses for the results of Mystery Shopper testing. Much use may be made of it internally in the agency conducting the process. It is also possible that other departments may require reporting in order to formulate new legislation or guidelines.

An additional use may be for punitive action against financial institutions in order to force or encourage compliance. If this is the case then the reports may need to be in a format that is acceptable to the court or tribunal or group to whom that the matter will be referred .

## Corrective Actions and re-testing

A fundamental aspect of the testing process is the formulation of corrective action to address shortcomings and weaknesses in the national AML system .

Corrective action could take a vast array of forms and might include such things as prosecution or regulatory action to force compliance –like licence cancellation or restriction, legal undertakings, deferred prosecution agreements etc. New laws may be required to prevent exploitation of new technologies, loopholes or new typologies. Improved education of financial institutions may be required to ensure that financial institutions understand their obligations. Alternatively, testing may highlight that financial institutions do not have access to the information required – such as PEPs lists, convicted offender lists, strategic intelligence etc that would be required to effectively identify high-risk behaviour and situations.

Clearly, following any corrective action the system must be re-tested to ensure that the desired result has been achieved. There is an argument for making re-testing as similar to the original test as it possible to assist with comparing results and allowing for changes to be attributed to the corrective action taken.