Abstract
This white paper explains the risks banks face when engaging with high-net-worth individuals (HNWIs) and how to implement an effective anti-money laundering (AML) program for wealth management and the program’s specific components.
Executive Summary

*The World Wealth Report 2015* states that the “robust economic and equity market performance” enabled wealth to grow by about 7 percent and has helped create nearly a million (920,000) new millionaires globally in 2014. This was the sixth consecutive year of growth for the high-net-worth market. Global HNWI wealth is projected to grow by almost 8 percent annually until 2017. The report found that the use of credit as a leverage for investments or equity financing in (HNWI portfolios is widespread.

HNWIs have shown keen interest in investing their wealth in areas which will drive a positive social impact. They are actively seeking help from their investment advisors to structure their investment portfolio in such a way that it will have a perceivable and measureable impact on their social efforts.

This growth in the economy has not only changed the economic risk factors, but has also affected the other macro environmental factors such as political, social, technological and legal risk influencing the finance industry.

The dynamic risk environment has created the need for the implementation of an effective AML program for wealth management. The key components of an AML program are risk identification, mitigating measures and governance which should be defined with a primary focus on HNWIs.

Proper governance is key to the success of any AML program. It is therefore important to stress the significance of AML by having top management explain the risk appetite to the organization. By doing this, a culture of compliance is created in the institution.

The growing threat of organized crime and terrorism continues to challenge the financial sector. Banks and financial institutions should ensure ongoing effectiveness of the AML program through periodic reviews and/or independent audits of the AML program.
Contents

1. Introduction.................................................................................................................. 4
2. Background...................................................................................................................... 5
3. Components of the AML Program.................................................................................. 6
   3.1 Risk Identification..................................................................................................... 6
   3.2 Mitigating Measures................................................................................................. 8
   3.3 Governance............................................................................................................. 10
4. Conclusion...................................................................................................................... 12
5. Glossary........................................................................................................................ 13
6. Bibliography................................................................................................................... 13
7. Annex (Case)................................................................................................................ 14
1. Introduction

“Don’t laugh, the piggy bank strategy works” reads an article dated April 20, 2014 in USA Today. While the Chinese consider the piggy bank a good luck charm, Europeans see the piggy bank as a harbinger of good fortune and wealth.

Wealth management works on the principle “save and invest” followed by growth, which ensures protection from inflation and returns on investment. Invariably, the elite community of the society or (HNWIs with more than $1 million in financial assets is defined as the target market. Banks further classify them as “hereditary HNWI and new money HNWI”—the former being individuals who inherited wealth and the latter being the new generation individuals who created wealth through opportunities provided by economic expansion and lucrative business.

How does this strategy work?

The wealth of these HNWIs would typically include fixed deposits, investment in mutual funds or balance available in the savings account. Banks appoint dedicated wealth managers or investment advisors to understand the risk profile of these clients and their immediate and long-term wealth goals. Based on these details, they offer products such as fixed income securities, equities or platform products and structure the investment portfolio. Once the portfolio is built, they monitor the performance of the securities and propose strategies to enhance returns from the portfolio.

This investment strategy and service excellence also attracts politically exposed persons (PEPs). These clients pose higher money laundering risk to banks due to the larger amounts they have available (to deposit or invest) and the ease of fund movement the privileged facilities allow them. Hence, the implementation of a strong AML program for wealth management is critical for banks and financial institutions throughout the world.

This white paper discusses the key components of an effective AML program for wealth management. It provides insight on the control framework required to mitigate the various types of risks the financial institution is exposed to during the tenure of customer relationship (HNWIs) along with the responsibilities of the three lines of defense. The mitigation measures are based on the author’s experience in the UAE, a country strategically located on the cross roads of Asia, Europe and Africa with diverse nationalities and a vibrant culture. The governance plan helps the assessment of program performance, periodicity of execution and enhancements related to developments in the AML field.
2. Background

In order to provide their clients (the HNWIs) with a broad range of investment products, banks enter into agreements with third-party providers. The provision of privileged services coupled with customized investment products or securities through these international players provides an attractive proposition to money launderers. In addition, certain banks provide their clients with a leverage facility which is primarily financing for the investment amount. This leverage facility exposes the banks to a high degree of credit risk.

The securities market has certain features which make it potentially vulnerable to money laundering:

- Large volumes of transactions with substantial transaction values can be executed rapidly
- Settlement transactions are also quick
- Commingling of clean and dirty funds is possible
- The use of cash to purchase securities is possible
- Where a number of financial institutions are involved in a transaction, customer due diligence (CDD) measures may have been missed by the institution initiating the transaction due to reliance on the other institutions involved in transaction execution
- Securities market manipulation and abuse of insider information
- The facility of opening Internet-based trading accounts

The evolution in money laundering techniques has resulted in dynamic risk factors challenging the financial sector. The 9/11 incident is a valid example of cross-border crime funded by high net worth and powerful individuals. This led the U.S. to mandate enhanced due diligence (EDD) for correspondent banking and private banking accounts maintained for non-U.S. persons. The Financial Action Task Force (FATF) also introduced new recommendations to jointly combat crime committed for money laundering and terrorism financing.

The source of wealth of HNWIs is varying. The changes in the profile of clients makes it necessary for financial institutions to recognize the emerging risks. Key risk factors which have significant impact on financial institutions when establishing an efficient AML program are mentioned next.

The comprehensive AML program for HNWIs shall include three components (i.e., risk identification [identification of various risk], mitigating measures [measures to control/mitigate the identified risks] and governance [validation of the mitigating controls/factors]).
3. Components of the Anti-Money Laundering Program

3.1. Risk Identification

3.1.1. Legal Risk

Legal risk is primarily the risk that would arise due to noncompliance with legislative responsibilities or violations of the law and may result in loss of reputation and/or penalties or imprisonment or sanctions imposed by regulators.

As per Basel III, legal risk includes conduct risk. Many conduct issues are a result of poor understanding or a lack of awareness of how legal standards (laws and regulations) apply to business operations, products and services.

In addition to providing quality service to their clients, investment advisors need to monitor market performance of the investment products and update their customers (HNWIs) to benefit from their investments. If they are not clear about their obligations and how these should be managed, the financial institution may face an uncomfortably high risk of reputation loss. Furthermore, when regulators announce multimillion dollar fines for AML violations, financial institutions will be burdened with stringent obligations to deter and detect money laundering and terrorist financing activities.

3.1.2. Political Risk

Changes in the political arena or political instability of a country have a major impact on its laws and regulations.

The 2011 political turmoil in Egypt subsequently escalated into political violence and damaged the country's economic outlook and investment returns. Thereafter, investors started withdrawing funds in search of safer havens. Political risk is dynamic with the changes in the political scenario.

Political decisions taken by government officials can affect business conditions and profitability. The political decision to uplift sanctions would enable Iran to join the mainstream global trade and financial system resulting in the expansion of trade and increased investment opportunities across the gulf. The increase in investment opportunities would attract HNWIs, however, the free flow of money would make way for unscrupulous players to funnel ill-gained funds into the economy.

3.1.3. Environmental and Social Risk

Environmental risk refers to the impact of natural disasters on humanity such as pollution, famine, tragedy, floods, earthquake, etc. Post such events, big foreign donors/HNWIs and non-governmental organizations (NGOs) are utilized by criminals as channels to divert the aid amount received from the government to finance terrorism and promote money laundering.
Social risk generally results in reputational risk for financial institutions. Reputational risk occurs when the clients of the financial institution engage in activities which present potential threat to the environment or society.

3.1.4. Economic Risk
Government regulations related to the finance or economics of a country may expose the investment portfolio to economic risk. However, economic growth drives the gross domestic product. A free and healthy economic regime fosters trade, which in turn creates wealth and enhances individual spending power. Economic growth also attracts money launderers who may sneak into the economy through the private sector. Please refer to the Annex for a live case involving HNWIs.

3.1.5. Technological Risk
Technology enables the key processes that an institution uses to develop, deliver and manage its products, services and operational activities. Since it supports the various business functions and drives the core business operation, technological risk is inherent throughout the institution.

Sophisticated services such as Internet banking facilitates account opening with fake IDs, which is a common technique used by cybercriminals who move funds across different jurisdictions to obscure the link between the criminal proceeds and the underlying criminal activities. Hackers and cybercriminals target alternate payment systems to siphon funds by diverting genuine transactions to their own accounts.

3.1.6. Credit Risk
Credit risk is the probability of monetary loss due to a borrower’s failure to repay the debt. For banks, loans are the most obvious source of credit risk and can pose a very high risk of money laundering. Loans can also be offered to wealth management clients via provision of leverage by the institution offering the Investment products. The leverage facility is also susceptible to money laundering as illegal funds could be used to prepay or settle the leverage amount.

3.1.7. Operational Risk
Operations risk is the risk resulting from inadequate or failed internal processes, people and systems and from external events.
Non-documentation of processes and lack of business continuity planning can lead to financial loss. Inadequate systems or systems with no enhancements or built in controls could also be disastrous. Human errors and external factors such as frequent power cut or natural calamities may disrupt operational procedures.

3.1.8. Residual Risk
Risk that cannot be mitigated based on available resources is generally categorized as residual risk. However, it differs from institution to institution. Due to the wide geographical spread of its HNWI clients, an institute may not be able to reach them and do a complete due diligence on such clients, which may lead to higher risk.

3.1.9. General
In addition to the above mentioned risk factors, at a pragmatic level, some of the red flags observed in wealth management relationships that need to be addressed in the AML program are:

- Incomplete know your customer (KYC) information
- Account opened for nonresidents without documentary evidence for source of wealth
- Account for HNWIs with third-party power of attorney (POA) operation
- Unclear source of wealth for high-risk nationals and PEPs
- Business account for HNWIs with multilayer ownership structure, third-party POA or key contact person (KCP)
- Offshore entities located in jurisdictions with weak AML regime

3.2 Mitigating Measures
3.2.1 Legal Risk
The legal department which is responsible for the regular interaction of the institution's business operation with legal standards needs to:

- Conduct a comprehensive analysis of potential financial and legal exposures in the different jurisdictions in which the institution operates including the litigation culture and impact of adverse judgement, in order to minimize financial and reputational risk.
- Give special attention to the wealth management clients holding positions of authority/PEPs by analyzing their exposure to government approved development projects and related financial arrangements.
- Periodically review provider agreements and various kinds of formatted documentation used by the business unit in processing securities and the leverage facility, to ensure adherence to the legal framework, statutory and regulatory bodies.

3.2.2 Political Risk
- Manage threats arising from the political environment, in the markets in which the institution operates.
- Continuously monitor political developments on a global, regional and country level to counter unforeseen risks and protect the investment portfolio.
- Include information available on the public domain for PEPs in EDD reports.
- Seek clarification from the business unit if adverse information is found in order to assess the risk involved in the relationship and compare with the risk appetite of the institution, prior to proposing the case to senior management for approval.
3.2.3 Environmental and Social Risk

- To develop resilience to natural calamities and adverse publicity and incorporate in the institution's business continuity plan and enterprise risk management program
- To address the impact of these risks on the investment portfolio in the annual sustainability report
- To analyze how business customers conduct their activities, prior to being linked with their business transactions via provision of trade facilities
- Ongoing due diligence of NGO accounts to be conducted and large withdrawals to be subjected to submission of ledgers for funds distributed and spent.
- Accounts maintained for nonprofit organizations to be closely monitored for unusual activity and ownership structure/authorized signatories to be reviewed regularly

3.2.4 Economic Risk

- Diversify the investment portfolio or spread the risk by investing in international mutual funds, which includes stocks, bonds and money market funds
- Private investment companies to be regulated for adherence to the legal framework
- Institutions to perform EDD prior to onboarding private investment companies. Identify ultimate beneficial owners (UBOs).

3.2.5 Technological Risk

- Risk to be addressed holistically in the context of the institution's business strategy
- To monitor the architecture of the institution's networks to determine the interconnections with other internal and external systems
- Identify access points and critical junctures where security mechanisms need to be placed
- Identify system threats and vulnerabilities to provide the management with a better view of the technological risks challenging the institution’s operations
- Controls to be placed in the transaction monitoring system to assess performance. Verify if alert generation is in line with the preset scenarios and risk views. Ensure accuracy of the screening tools.

3.2.6 Credit Risk

- In-depth analysis of repayment capacity
- Customer profiling to include verification of source(s) of income including investments with other banks, real estate income, etc.
- Mortgage loan or leverage facility with other banks to be deducted from disposable income.

3.2.7 Operational Risk
System issues

➢ Fix efficient software to detect, monitor and analyze the risks arising from internal operations, processes, employees and systems
➢ To gain increased control and visibility over the entire financial process and minimize risk by proactively identifying the potentially expensive flaws

People

➢ Minimize human errors
➢ Follow correct procedures
➢ Recruit employees who are professionally qualified to perform the functions of the role
➢ Minimize infidelity by conducting a background check of employees before recruitment

Process

➢ Implement time tested and approved procedures to ensure seamless workflow and completion
➢ Identify deficiencies in the existing procedure or identify undefined procedure
➢ Review standard operating procedures periodically
➢ Suggest amendments based on experiences to improve procedures and to ensure effective operations risk management

3.3 Governance

The earlier mentioned mitigating measures should be exercised through a three layers of defense setup:
The first line of defense shall constitute the front-line business unit (wealth management business unit) that includes the investment advisors. They shall be responsible for:
➢ Implementing an effective KYC standard by adopting sound customer identification and verification procedures to protect the institution from legal and reputational risk;
➢ Adoption of enhanced KYC measures for nonresident customers, POA operated accounts, nationals of high-risk countries and PEPs. Nonresident individuals to be introduced by existing resident customer. Documentary evidence for source of wealth to be included in the KYC mandate;
➢ Identifying beneficial owners of legal entities. Probe underlying purpose of establishing companies with complex ownership structure involving multiple entities/holding company;
➢ Providing quality advice to their clients to manage the impact of economic risk, political and environmental changes and social consequences to the investment portfolio.
The second line of defense shall include the institute’s AML and compliance unit who shall be responsible for:

- Promoting a sound risk culture by regularly testing the risk awareness of the business unit and the controls placed to mitigate risk;
- Addressing the queries or issues raised by the investment advisors by providing regular training on risk identification and business impact without compromising on service quality and customer confidence, in order to mitigate conduct risk;
- Monitoring the performance of the transaction monitoring system to ensure continuity of the AML program and to minimize technological and operational risk;
- Ongoing due diligence of NGO accounts, nonprofit organizations and PEPs to minimize legal, political and social risk.

The third line of defense shall include the institute’s top management who shall decide and be responsible for:

- The institution’s tolerance for risks
- Fostering strong and enduring control culture and risk awareness throughout the institution
- Approve the AML program for the institute
- Approve onboarding of high-risk clients such as PEPs and nationals of sanctioned countries
- Explore the options for “transfer of risk” to third parties such as insurance companies.

### 3.3.1 Audit

In order to ensure the validity of the above risks and mitigating measures and governance, the same needs to be audited by an independent auditor. The broad framework of such an audit plan shall include:

- Objective (evaluation of adequacy and effectiveness of the AML program)
- Scope (AML program for wealth management)
- Testing (systems and controls)
- Report (observation, noncompliance)
- Recommendations (additional mitigates, remedial action plan, training needs)
- Periodicity (frequency of review)
4. Conclusion

An AML program provides the guidelines to essentially protect banks and financial institutions from money laundering risks, however, the evolving trends in money laundering techniques makes it next to impossible to cover all risks in full. Banks and financial institutions implement a risk-based AML program to cover these evolving AML risks.

Due to the extensive exposure to HNWIs, including PEPs, financial institutions require to execute an exclusive and robust AML program for wealth management. The key risk factors that could have a negative impact on the institution’s operational procedures need to be mitigated. In addition to the financial risk involved in the transactions related to securities and sophisticated investment products, new risks related to changes in the profile of HNWIs may appear every day.

The highlighted risks, the mitigating measures and the three-tier defense model forms the framework for the AML program and clearly defines the responsibilities of the wealth management business unit and the AML and compliance unit of the institution.

To keep up with developments in the AML field and the changing business environment, the AML program should be audited periodically by an independent auditor who needs to validate the mitigating measures and controls and record the findings and weaknesses. The audit report, with the required improvement measures and system enhancements, should be submitted to top management.

"Tone at the top" remains crucial in detecting and preventing the institution from crime and money laundering. Ultimately the board members and senior management is responsible for the AML compliance efforts of the institution and fulfillment of regulatory obligations. Similarly, they should take the responsibility of supporting, fostering and maintaining a strong culture of compliance in the institution."
5. Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>HNWI</td>
<td>High Net Worth Individual</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>UBO</td>
<td>Ultimate Beneficial Owner</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>NGOs</td>
<td>Non-Governmental Organizations</td>
</tr>
<tr>
<td>POA</td>
<td>Power of Attorney</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Due Diligence</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
</tbody>
</table>

6. Bibliography

3. [mint.com](http://mint.com)
4. [www.fincen.gov/statutes_regs/patriot/](http://www.fincen.gov/statutes_regs/patriot/)
6. [www.bis.org/bcbs/basel3.htm](http://www.bis.org/bcbs/basel3.htm)
7. Annex

Case

Shell companies are ideal vehicles for money laundering and other illicit activities. When these shell companies are held privately, beneficial ownership can be easily obscured or hidden. The below case which involves HNWIs explains how these private companies were abused for layering of illegitimate funds through the financial sector. Additionally the free-zone business model facilitated 100% ownership for the HNWIs.

The owner of a casino ring promised his HNW clients to assist them in growing their wealth by investing in the securities market of a country well-known for its lucrative business opportunities and high investment returns. A con man belonging to a poor country was hired to form multiple free-zone companies. Investment accounts were opened in the name of these companies in different banks with the con man as the Key Contact Person / Authorized signatory. Securities were purchased and redeemed prematurely within few months followed by transfer of the proceeds from one bank to another. Finally the funds were placed in short term fixed deposit and wired back to the respective company accounts.