Financial payments have seen a new wave of technological advancements with the emergence of e-payments or alternate payment methods (APMs). These instruments increase concerns over money laundering and terrorist financing as the new, technologically advanced channels can be exploited by miscreants.

While organizations are increasingly aware of the risks inherent in alternate payment methods, they are also wary of the fact that these methods have significantly augmented their business growth across geographies. Risk mitigation using effective countermeasures by means of an integrated, enterprise-wide 'governance, risk and compliance' strategy, is the way forward.
What are alternate payment methods?

Traditionally, financial payments have involved cash or cash-derived instruments for funding. The advent of new technologies has seen the emergence of a host of APMs like the Internet, mobile telephony and card-based instruments, all of which are rapidly finding acceptance worldwide. Cards were the first among the non-cash instruments to witness widespread usage in retail payments. With the dawn of the Internet era, online fund transfers have slowly started stealing the limelight that debit/credit cards used to enjoy. The mobile channel is now creating a wave in payments and related spaces.

While the advent of technology is one aspect, the movement of many financial operations out of the ‘typical’ bank is another important aspect in defining these APMs. Today, non-banking entities provide multiple services all the way up the value chain, right from payment initiation to settlements. A case in point is certain types of mobile payments or ‘m-money,’ wherein pooled accounts are maintained by the service provider and the bank functions merely as a conduit for handling the transfer and settlement without directly interfacing with the customer.

In essence, an APM includes the set of non-cash and related instruments that could be linked to an underlying banking product or otherwise, and used to perform a financial payment towards services, products or other financial transactions. Some of the alternate payment methods include Internet payments, mobile payments, pre-paid cards, electronic purses and digital precious metals.

Alternate payment methods

- **Internet payments** include payment services that are performed on the Internet channel for funding bank or non-banking transactions.

- **Mobile payments** are a set of financial transactions conducted using the mobile phone.

- **Pre-paid cards** are pre-funded instruments issued to customers for specific or generic payment utilities.

- **Electronic Purses** are instruments with the value stored on a pre-paid card.

- **Digital precious metals** are derivative instruments that can be transferred to other individuals or used to make payments in exchange of goods or services.
What differentiates alternate payment methods from the traditional methods?

PAYMENT SERVICE PROVIDER
Since traditional payment services are either cash or negotiated instruments as provided by the bank, the service provider is always a financial services provider. In the case of APMs, it could be a bank or a non-banking institution that provides the service.

Typically, for payments channels that are extensions to traditional systems wherein payment services are based on an underlying banking account, the bank will be the service provider. For instance, Internet banking, mobile banking, pre-paid payment cards, etc. operate on a banking account. For new payment systems—like m-money, calling cards, Internet-based funded accounts—that are not based on an underlying banking product, the service provider need not always be a banking entity.

ORIGINATING CHANNEL
This is the most important and visible distinguishing factor for the end consumer. The channels for APMs tap into newer methodologies like Internet services, mobile applications, etc.

SETTLEMENT
While the financial settlement entity might remain the same in traditional and non-traditional payment channels, the settlement terms could vary drastically. Internet and mobile services enable immediate access to funds and provide for a broader array of services for the end consumer to choose from. In some of the models of alternate payments, banks are not involved in consumer account settlement and only perform the final settlement on the pooled account held by service provider or merchant.

USAGE
APMs can typically be categorized as open system or closed system instruments. Open system instruments permit transactions with accounts or services that are not part of the system and can be compared to any other traditional instrument where usage is not restricted. Closed system APM instruments, on the other hand, let the user perform transactions within the boundaries of a defined system, hence restricting usage.

Can APMs be misused for money laundering purposes?
The emergence of alternate payment methods has brought in a lot of advantages vis-à-vis traditional modes of payments.

Advantages of APMs

- Lesser use of cash transactions
- Improved trace of money movement
- Stronger implementation of regulations
- Increased reach
- Better financial inclusion
But financial payments, be it traditional or non-traditional modes, have an inherent money laundering/terrorist financing (ML/TF) risk. The following chart depicts those risks by highlighting APM-specific factors when compared to traditional payment systems.

**ML/TF risks associated with APMs**

- **PAYMENT SERVICE PROVIDER**
  - Range of service providers is vast and account and transaction monitoring procedures can vary
  - Service providers provisioning offshore accounts increased the risk as the degree of money laundering/terrorist financing regime can vary between countries

- **ORIGINATING CHANNEL**
  - Internet and mobile technologies make transaction activities more elusive. Smurfing money for criminal activities can be spread across geographical boundaries
  - Transactions on newer channels occur in real-time, leaving banks and authorities with very little time to stop suspicious activities

- **SETTLEMENT**
  - In closed system transactions, banks need not be aware of the questionable activities within these accounts as they might be exposed to activities at only the pooled account level, and not between accounts
  - Due to quicker access to funds, suspicious, high value transactions cannot be immediately flagged by the system

- **USAGE**
  - Open system instruments with no limits on geographical boundaries could make jurisdictional authority ambiguous
  - APMs with no value limits and allowing anonymous payments pose a significant risk of money laundering

A strong risk & compliance program coupled with vigilant governance is a direct requirement to combat this all-pervasive risk. Every country has its own set of regulations to restrict, monitor, report and govern financial transactions based on varying contexts. However, given that governments all over the world, especially the developing world, are striving towards financial inclusion and growth, it is crucial that anti-money laundering/countering financing of terrorism (AML/CFT) programs not be so rigid as to curtail the free and fair financial transactions undertaken by the majority of the people.

As per the analysis and research done by various bodies such as Financial Action task Force (FATF) on new payment methods, GSM Association (GSMA) on m-money, APMs can pose a significantly lesser risk as compared to cash transactions because of the electronic trace of the transaction it leaves behind. At the same time, criminals are always coming up with newer methods of laundering money by exploiting loopholes in technology and governance. This ML/TF risk can be minimized by understanding the transaction flows of various channels and potential weaknesses of these systems, and addressing the same with optimal and effective controls.
Analysis of transaction flows in APMs

The emergence of alternate payment methods has brought in a lot of advantages vis-à-vis traditional modes of payments.

Service provisioning
Alternate payment methods get their characteristics by the service provider offering the service over a specific instrument or channel. Hence, this would be the significant entity in the transaction flow and defines the very nature of the financial transaction. Service providers could be banks, mobile network operators, merchants, Internet services, etc., who make provisions for payments within the system.

THREATS:
- Open system or multi-purpose cards can be used across a broader range of locations and purposes
- Telecom operators and other non-bank service providers might not be directly overseen by the regulators
- Verification activities of service providers may not be comprehensive or uniform
- Channel-specific loopholes like network-related frauds and transaction content anomalies are rampant in Internet and mobile-based payment services

Customer interaction
This essentially refers to the interface that connects the customer to the service providing entity. When a financial transaction is performed on non-traditional payment instruments, the nature of customer interaction varies widely. The various mechanisms of customer interactions could be Internet-based transactions, mobile-based transactions and transactions at retail outlets.

THREATS:
- No face-to-face identification or relationship with the client
- Improperly identified or anonymous accounts are potentially high risk
- Anonymous account funding and receipt of funds
- Authentication and authorization-related issues like account hacking could be misused for money laundering purposes
Transaction processing

This is a middle office operation wherein transaction instructions are converted to actual processing. Any transaction performed on a certain instrument or channel will have certain characteristics, such as transaction amount, beneficiary and settlement terms, to facilitate its processing. Additionally, there are certain account traits like usage limits, fund limits, business terms, compliance terms, etc. that need to be validated before this transaction is performed. Once the feasibility of the transaction is determined, the transaction can be processed and account records updated accordingly.

THREATS:
- Verification of authenticity of the third party might not be possible in open system APMs
- Blurring jurisdictions in Internet-based transactions can result in governance issues
- Offshore service providers may not be compliant with regulations of other jurisdictions
- There could be some manual transaction processing, in which case velocity checks will be difficult to track
- Non-existent account and transaction level limits

Account provisioning

Account record keeping is a very important activity in any financial transaction process. Based on the mode of operation of the APM and its specific implementation, account provisioning can be performed by different types of entities. For instance, Internet service provider Paypal maintains the customer accounts and the bank is only needed for final settlement. Whereas, in the case of some m-money services, the mobile network operator only provides the channel for user interaction while the account maintenance rests with a banking entity. It can be deduced that the kind of account attributes maintained and the duration before archival could also vary based on the entity responsible for the account provision.

THREATS:
- Pooled accounts make it difficult for financial institutions to track individual transactions
- Maintenance of transaction history may rest with multiple entities and consolidated information might not be available

Transaction settlement

Settlement in the case of APMs has taken a new definition owing to the entry of non-banking entities in the lifecycle of transaction processing. Banks that were required to perform customer account settlement are now increasingly playing the role of a final beneficiary as an increasing number of service providers reconcile the accounts themselves and maintain pooled accounts with banks.

THREATS:
- Newer technologies have brought in immediate counter-party settlement, which, in turn, poses a higher risk of money laundering
- Settling banks may have no link with customers and hence regulatory compliance becomes difficult to impose

While each of the above processes is integral to a transaction performed using APMs, the segmentation of services is one of the biggest challenges to address. Several independent service providers executing different steps in the transaction lifecycle is a viable option for businesses, but without effective interaction between service providers, the risk of ML/CFT increases manifold. Oversight of these segmented services is a challenge in itself, which gets exacerbated by service providers outsourcing services without taking proper measures to set out lines of responsibility amongst themselves. The solution proposed for this is a unified mechanism of risk management, compliance checks and end-to-end governance applied across the value chain.
ML/TF risk mitigation strategies for alternate payment methods

It is established that APMs are not void of ML/TF risk factors. To counter and mitigate these risks, regulators the world over have left no stone unturned to bring in tighter controls. Different geographies have come up with different strategies to address regulatory challenges for these new payment methods. In European countries, some payment services have been restricted only to financial services, which make it easier to regulate. In India and Australia, some forms of APMs, such as digital precious metals, are restricted for trading, thus reducing the associated risk. The United States recognizes any non-banking institution offering payment services and regulates them under various regimes. There are special laws governing payments made through online payment service providers based outside the country. One of the key factors to note is that the penetration of APMs varies across geographies and has reached different levels of maturity. While developed countries have evolved a unified approach to regulation across all channels, developing countries have evolved regulations in a highly diverse manner. This inherently increases the risk of ML/TF.

From a transaction perspective, each of the stakeholders involved in payments that use an APM instrument needs to exercise some safeguards to comply with regulations and reduce identified risks. The following are risk mitigation practices that need to be implemented by payment service providers and other entities in different forms.

**Customer due diligence**

Due diligence of the customer entering the system is the first step towards mitigating risk. This objective is achieved by employing a two-step process—customer identification and verification. For all practical purposes, these can be achieved through know-your-customer (KYC) and enhanced due diligence (EDD) measures.

The identification step involves identifying the customer at the start of the relationship, maintaining an ongoing assessment of the customer and determining the beneficiaries of transactions performed by the customer. KYC processes usually check the true identity of the customer with regard to various factors such as location, nature or business, criminal background, political background, etc. Based on the type of APM, the details required for checks will differ. While KYC for online merchandise payments may not be as rigorous, the identities of both the originator and beneficiary need to be ascertained for any other type of third-party payment.

The verification step deals with the other aspect of due diligence, namely, ensuring that the identity claimed is authentic and not an impersonation. Achieving this involves an EDD policy that encompasses in-person residence checks, comprehensive background checks, and IP checks for online transactions.

**Transaction limits**

Imposing limits on transactions is required from both, compliance and business standpoints. There could be various types of limits set—value limits, geographic limits, funding limits, usage limits, etc. Setting appropriate limits pertinent to the business context is the key to efficient control.

- Value limits discourage users from performing high value transactions. This could include transaction-level limits, account-level limits and account-funding limits.
- Applying geographic limits or restricting usage of APMs to the national boundaries makes regulation easier. In online
payments where this cannot be achieved, suitable network access checks and IP checks can be exercised to augment geographical checks.

- Usage limits are, more often than not, determined by the type of APM and the service provider offering the service. Closed system instruments are restricted in usage owing to the definition of such an instrument. Open system instruments that have access to cash need to be coupled with pre-specified value limits and defined utilities to reduce risk.

**Transaction monitoring**

While effective onboarding is important for assessing customer risk, continuous monitoring of transactions is indispensable. AML programs cannot be complete without suspicious activity monitoring, surveillance and investigation. This will be of more relevance to APMs since transactions carried out using these non-traditional methods usually leave an electronic trace, which can then be analyzed.

Monitoring can be carried out on:

(a) Individual transactions for anomalies
(b) Set of transactions for abnormal patterns
(c) Historical transactions for behavioral patterns
(d) Linked transactions for corroborating network patterns

These objectives can be achieved by processing the details pre or post settlement, as the case may be.

**Record keeping**

Record keeping is another important yet downplayed activity in AML programs. Transactions can be monitored effectively only if account records are up-to-date. APMs with segmented services specifically need the transaction activities to be updated regularly as there are multiple parties like issuers, distributors, retailers, agents, banks, etc. Without a clear demarcation and record of activities performed at each level, it gets very difficult to detect the presence of abnormal activities.

**Oversight**

Lastly, the single most important driving force behind the AML/CFT regime is oversight by the business, regulating body and government. At the first level, every service provider has to oversee the transactions under its purview as prescribed by the regulator. Poor oversight may intensify other systemic risks of APMs. AML laws comprising of unified KYC norms are largely increasing their scope to regulate new-age payment systems. Governments need to actively participate in forming regulating bodies for different operations and determining their scope. For instance, mobile money can be partly overseen by the telecom authority of a country that may not be well equipped to handle AML/CFT procedures. Effective governance to plug these loopholes will not only reduce money laundering but also facilitate business growth.

Beyond regulation, financial institutions also need to actively monitor and report the usage of APMs to better evolve and spread the use of non-cash modes of payments. In conclusion, there needs to be a bottom-up approach to ensure adherence “in spirit and letter” to the regulators’ attempt to provide a manageable, limited risk environment that allows the greater proliferation of APMs.

---

**Integrated governance, risk and compliance (GRC) model for risk mitigation**

**Need for an integrated GRC**

Initial technology solutions focused more on KYC requirements and paid less attention to the transactional monitoring aspects of AML. Financial systems always considered AML to be a regulatory compliance function that is handled separate from internal risk management systems. However, ML/TF inherently puts institutions/countries at risk, due to which it makes greater sense to integrate risk management and compliance functions. Regulators have also been active to ensure that the laws are upgraded to deal with newer threats emerging from APMs. As a result, governance requirements have consistently gone hand-in-hand with regulatory reporting in most jurisdictions. In this environment an integrated GRC solution is more relevant than having silos for each of the above requirements.

**Governance** addresses setting up of business objectives, functional strategy, formulating internal policies and measures, and assessing the same by suitable parameters to ensure adherence to laws of the land and international laws. Most governments, financial institutions and businesses alike target inclusivity of all strata of the society. Usage of APMs ensures wider reach and better access to payment instruments for all sections of society. In doing so, AML/CFT policies should be formulated to ensure effectiveness and efficiency of operations with optimal internal controls.

**Risk management** deals with the process of identifying internal and external system-related uncertainties, formulating a risk mitigation strategy and managing the identified risks in order to achieve desired business objectives and gain a competitive advantage. Customer and portfolio risk assessment, profiling, risk treatment, risk management frameworks and finally, periodic reviews, are some of the broad components of risk management. With the advent of new technologies, it is critical that organizations understand the systemic risks inherent in financial transactions and their impact on the overall business.

**Compliance** is the desired state of operation in sync with the business objectives, the laws and regulations of the land and stakeholder commitments, achieved by adapting policies and procedures on a day-to-day basis. This includes a broad range of regulations and business policies that are formulated to bring about a positive effect on the overall economy and actively promote use of a wider range of financial services using different payment methods while ensuring transactions with money laundering motives are effectively tracked and eliminated.
The previous section has put forward strategies that can be leveraged to reduce the risk of ML/TF activities through APMs. But these strategies are bound to be ineffective without a proper compliance framework and internal controls. With financial payments becoming more sophisticated and diversified, a robust internal control program is the need of the day. The lack of a coordinated GRC program can lead to inconsistencies in business operations.

**The need for an integrated GRC model**

An integrated GRC policy is designed to define the processes and structures of the organization in implementing a unified business framework as defined by compliance laws and internal alignment to operational practices. A strong GRC program enables businesses to integrate unorganized, disjoint and isolated programs, processes, and systems into effective and efficient strategic, enterprise-wide, risk-based control structures.

**GRC objectives**

In the context of AML/CFT, the key objectives of integrated GRC model are:

- Defining the business objectives on AML/CFT or organizational risk
- Formulating policies and defining processes for operations
- Defining risk objectives, tolerance and contingencies
- Assigning governance roles and responsibilities
- Stakeholder communication and training
- Implementing risk and compliance framework through continuous monitoring
- Operational reporting and controls
- Regulatory reporting and investigation

The various GRC activities as seen in a GRC framework are depicted in the figure below.

**GRC activities for AML/CFT**

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
<th>RISK MANAGEMENT</th>
<th>COMPLIANCE MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT objectives</td>
<td>Customer due diligence</td>
<td>AML/ CFT regulations</td>
</tr>
<tr>
<td>Policies and processes</td>
<td>Intrinsic risk management</td>
<td>Know your (KY’X’)</td>
</tr>
<tr>
<td>Role and responsibilities</td>
<td>Controls monitoring (value, funding limits)</td>
<td>Watch list screening</td>
</tr>
<tr>
<td>Risk definition and risk tolerance</td>
<td>Behavioral risk management</td>
<td>Suspicious activity monitoring</td>
</tr>
<tr>
<td>Audits &amp; reporting</td>
<td>Transaction monitoring</td>
<td>Exception management</td>
</tr>
<tr>
<td>Dashboard and operational reporting</td>
<td>Employee monitoring</td>
<td>Regulatory reporting</td>
</tr>
</tbody>
</table>
Solutions for implementing a GRC framework

Implementation of risk and compliance management solutions is an expensive and complicated undertaking that is subject to periodic changes. At the same time, deficiency in regulatory compliance could result in penalization and reputational loss while non-adherence to business objectives and risk methodologies could result in hampered growth.

Significant changes are being witnessed in the way services are delivered by financial institutions to end customers. APMs have transformed the way services are delivered but they are not foolproof and prone to high risk of fraud. Financial institutions are always in need of an effective GRC framework that can bring down financial losses and, at the same time, ensure a highly configurable system that can rapidly adapt to newer technologies and related regulations.

A strong and agile integrated GRC solution is the need of the hour. Financial surveillance systems catering to GRC space can be categorized based on the various levels of maturity.

### Maturity levels of GRC implementation

**Level 1:** This is the initial level of compliance with fragmented implementation of monitoring and detection. There could be inconsistent, redundant and duplicate operations resulting in increased effort on part of a centralized team to manage and provide an integrated view to the management. Processes might not be defined at an organizational level for risk assessment and treatment, and compliance management.

**Level 2:** This level indicates well-defined organizational policies and structure for overseeing the multitude of compliance programs that might be running within the organization. Co-ordination between various programs is better, which results in lower operational costs.

**Level 3:** The organization has a well-managed and governed GRC implementation that is process oriented and caters to the organizational and compliance policies, which are administered centrally. This aims to provide a single view of compliance and relies on technology to bring about measurable guidelines for GRC implementation.

**Level 4:** This is a truly integrated GRC framework whose aim towards compliance is that of continuous functional improvement. GRC policies are planned and governed at the organizational level, managed by central teams, administered to relevant departments and customized to suit diverse requirements. This brings about a unified strategy for harmonizing various levels of fragmentation viz., organizational, system-centric, and geographical policies.

GRC solutions themselves have metamorphosed to suit the changing GRC implementation necessities of customers.

### Metamorphosis of GRC solutions

- Standalone compliance solutions
- Independent regulatory reporting
- Risk management
- Transaction monitoring
- Integrated GRC principle
- Behavioral detection
- Learning engine driven
- Business Process Management
- Integrated governance principle
- Cross-functional applicability
- Fraud management
With the advent of new-age APMs, GRC solutions generally aim to bring about a Level 4 value to customers by bringing solution suites to help financial institutions comply with AML regulations from regulatory agencies around the world. They are designed to be agile, multi-faceted and adaptable to constantly-changing business demands.

To meet these demands from customers, GRC vendors are now offering IT GRC and moving towards an enterprise GRC that involves consolidation of various IT programs in itself. They deliver competitive offerings with a wider range of next-generation feature sets, including:

- End-to-end AML solution
- Highly configurable to suit specific business requirements
- Suspicious activity monitoring by means of behavioral detection principles
- Adaptable solution with self-learning techniques
- Cross-channel fraud detection techniques
- Workflow-driven compliance processes
- Integrated investigative case management
- Dynamic and interactive reporting

Customers can choose from a wider range of products with niche offerings to the ones built for providing an enterprise GRC capability. Speed and adaptability to technology are two pillars of GRC solutions that are bound to be differentiating factors between various offerings. Speed at one hand indicates the ability to bring solutions for new regulations, configurability, time-to-market and implementation time while, on the other hand, symbolizes the velocity with which the solution keeps pace with criminal activity and early detection techniques. Adaptability refers to changes in the solution as a consequence of changing regulations, technologies, methodologies, business needs, people and processes. A GRC solution that embodies the principles of enterprise GRC by quickly adapting to the speed of criminal innovation will be a clear winner.

In today’s world, new, cutting-edge technologies are bringing about a fundamental change in the way financial transactions are processed. Payment methodologies built on these technologies, also called alternate payment methods in this paper, are faster, sophisticated and offer an extremely efficient system for doing business. Criminals have made use of the untapped and less trodden areas of these technologies and managed to be one step ahead and more advanced than the governing systems. The use of advanced technologies has resulted in enhanced risk as compared to traditional payment modes. As a consequence, financial institutions are in dire need of monitoring and surveillance systems to ensure better risk mitigation. At the same time, these compliance systems need to be intelligent enough to take a call on various degrees of surveillance and investigation so as not to hamper business growth.

In the wake of increased technological awareness and complexity of money laundering methodologies used by criminals, surveillance systems are but expected to detect ML/TF crimes effectively. These next-generation systems are now a reality due to the evolution of compliance principles and onset of integrated governance, risk and compliance management. GRC vendors today offer a wide array of out-of-the-box capabilities that are intelligent, adaptive and proficient. With such systems becoming better by the day, one can only envisage a safe and sound infrastructure for financial transactions done by the common users.

References
6. ‘Know Your Customer: Quick reference guide’, PWC, Also available on http://www.pwc.com
About the Authors

Sowmya Nadig
Experience: 9+ years
Domains: Banking, capital markets and IT domains with a specific functional focus on governance, risk and compliance (GRC), brokerage and retail banking.
Strengths and achievements: Sowmya has an extensive experience in product ideation, strategy and pre-sales in IT product solutions as well as development, management and implementation of services for various clients. She has been actively involved in building trade compliance, AML and KYC methodologies for FSI products.
Contact: She can be reached at Sowmya_Nadig@infosys.com

Ananda Sreekanta Murthy
Experience: 16+ years
Domains: BFSI IT products solutions – Anand has built, implemented and supported products across the core banking, investment banking, trading systems, Islamic banking, microfinance, GRC, insurance, and enterprise data warehouse areas.
Strengths and achievements: Prior to Infosys, he was head of the products division of an Indian BFSI IT products company where he managed the development, implementation and support of various product lines. Anand was involved in building and implementing some of the first AML solutions as far back as 2001 in LATAM. He also recently transformed a leading AML solution into a compliance and financial crime surveillance solution, which helped re-position the product in the market at double the license price.
Contact: He can be reached at Ananda_Murthy@infosys.com

About Infosys
Infosys partners with global enterprises to drive their innovation-led growth. That’s why Forbes ranked Infosys 19 among the top 100 most innovative companies. As a leading provider of next-generation consulting, technology and outsourcing solutions, Infosys helps clients in more than 30 countries realize their goals. Visit www.infosys.com and see how Infosys (NYSE: INFY), with its 150,000+ people, is Building Tomorrow’s Enterprise® today.

For more information, contact askus@infosys.com www.infosys.com