Success Through Transparency

September 2021

Success Through Transparency

Know Your Partners

Successful participation and growth in the mobile ecosystem, whether your segment is messaging, digital payments, identity services, internet of things, or other value add services, requires trust between customers and providers at all levels. If the consumer can be confident that they know who they are hearing from, buying from, or trusting with their information, they will answer the call, respond to the message, complete the purchase or provide the data that allows the ecosystem to thrive. It is therefore incumbent upon all stakeholders to ensure the integrity of the partners in the value chain.

While some partners in mobile services are large, well-known public companies with global reputations that precede them, most brands reaching out to customers over mobile are likely to be relatively small unknown players pitching lesser-known products or services in which consumers have no pre-established trust. Though most businesses honestly seek to deliver value, a small but powerful minority of nefarious actors inevitably upset the marketplace by betraying trust and defrauding merchants, content service providers, mobile network operators, and consumers.

The transparency that spoils the game for the bad actors comes in the form of careful consideration and verification of the value chains entering the ecosystem (brand plus all interim resellers and aggregators), diligent review of the content and products offered to consumers, and ongoing monitoring of reputation and in-market behavior.

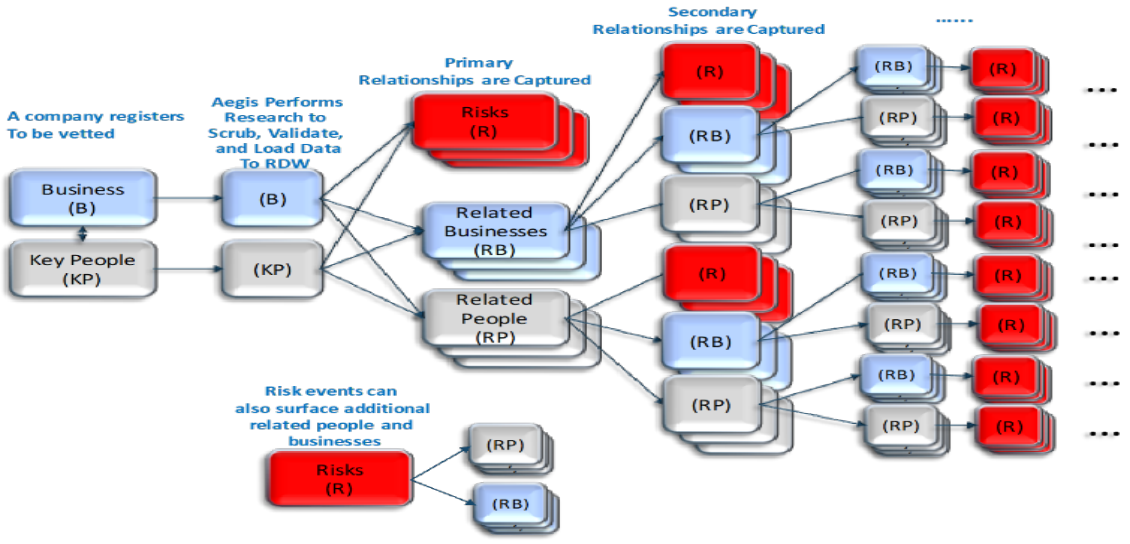
Since the large number of stakeholders and products in the mobile ecosystem appears daunting at first, the industry's capabilities and techniques have evolved since the early days of messaging, using the power of APIs, big data, large-scale real-time network monitoring, machine learning and artificial intelligence. Such technologies, in combination with networks of dedicated experts in the field, yield the ability to identify, avoid, and mitigate risks in these complex markets.

A full life cycle compliance approach begins during initial engagement between stakeholders and continues through and even beyond the retirement of stakeholders and their content. Throughout the life cycle, continuous learning and improvement must be applied to stay current with the evolution of risky behaviors, techniques, and technologies.

The first step in engagement between potential stakeholders is getting to know the other party (Know Your Customer – "KYC," or Know Your Partner – "KYP"). The process of conducting due diligence is often considered a strictly legal or contractual matter, but experience indicates that it needs to be a process tailored to your product and ecosystem to be effective – both in cost, level of assurance and risk avoidance.

The Know Your Customer (KYC) Process

The KYC process is an investigation of a potential partner, their related companies, their key employees, and the identification of any risk events associated with these companies or key employees. The following model depicts how complicated the KYC linkage can become for a complex business entity.



All businesses have key business personnel and may also have related companies that have key personnel as well. If we define the combination of companies and key personnel as Entities, we are then looking for relevant risk events tied to each entity and risk scoring these events back to the company that has registered to join the ecosystem. The older the risk events, and the further away from the company being vetted, the lower the impact to the overall risk assessment.

What is Risk

As a KYC best practice, risk is defined by the ecosystem, the business use case and the laws, regulations, and policies that govern the business channel. In most instances it is those who can be most impacted by legal and regulatory matters in the event of bad actors harming consumers who should drive the definition of risk as it pertains to KYC. Each industry will weigh the importance of risk categories differently. An illuminating example is the surety industry that underwrites bail bond companies, in which we have found the need for the unique treatment of a type of risk associated with key executives. The officers or owners of a bail bond company are often past or honorary members of gangs or may have been incarcerated on multiple occasions.

Traditionally those characteristics would be judged as presenting high integrity risk. However, in the surety industry these “risk indicators” are considered key to generating a strong book of business. Being a member of a gang increases both number of contacts and customer trust if you are selling bail bonds. While the differences between other industry needs is usually more subtle, this serves as a dramatic example as to why different industries have their own unique sets of relevant risks as well as weighting methodologies assessing risks in their KYC programs.

The table below shows a summary of risk category types. Each risk type can drill down to hundreds or thousands of individual events that an investigation process must identify and then assign a value to be used in quantifying the overall risk associated with each company. A consistent risk evaluation and scoring methodology must integrate variables such as years in business, business size, frequency, outcome, and more. Structure and consistency with evidence of the results are key to a successful KYC program.

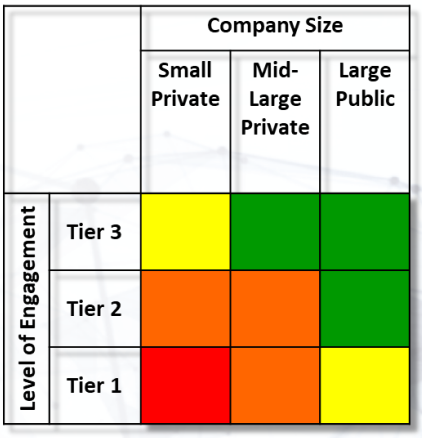
Sample Risk Event Types

Criminal	Legal	Financial	Ethics	Safety	Regulatory
Violent Crimes	Contracts	Money Laundering	Human Rights	Health	Advertising / Marketing
Property Crimes	Property	Tax Evasion	Environmental	Terrorist / TSA	Credit and Finance
Inchoate Crimes	Civil Rights	Securities Fraud	False Billing	Sex Offender	Privacy and Security
Statutory Crimes	Forfeiture /Penalty	Racketeering /Bribery	Data Privacy	Environmental	Regulated Industries
Homocide	Other Statutes	Financial Fraud	Labor Law	Product	Communications
Cybercrime	Tax Suits / Bankruptcy	Bankruptcy / Leans	Consumer Fraud	Child Labor / Work Conditions	Trade

Entity Risk versus Risk Exposure

KYC considerations differ according to the type of partner, the engagement you expect with the partner and potential risks that engagement presents to your product, its users, your reputation, and your operations.

The following examples of inherent risk posed by various external parties will help illustrate this point.



Probability of Business Risk

- Low risk: Copy paper supplier (Tier 3)– doesn't represent your company's brand so low reputational risk even if they do something that causes harm. They are not engaged directly with your customers so there is no potential to hurt them. They do not interface with your systems so there is no cyber-risk. Overall, they present a relatively low value/expense so even if they defraud you, you will not lose much.
- Low-medium risk: Low volume messaging brand with no payments or PII use cases. They operate indirectly through your company's systems, so they present some peripheral reputational risk. They engage directly with your customers so there is some potential to do harm via unwanted messaging and scams. They have limited interfaces with your systems, presenting low cyber-risk. Overall, they present a relatively low value/expense, so low financial risk.

- Medium risk: Messaging Independent Software Vendor (ISV) or Content Service Provider (CSP) with no payments or PII use cases (Tier 2). They operate at high volume either indirectly or directly through your company's systems, presenting increased reputational risk. They engage directly with your customers so there is greater potential to do harm via unwanted messaging and scams at scale, increasing the need for diligent monitoring. They interface with your systems, presenting an increased degree of cyber-risk. The high volume of their operations presents higher financial risk potential as well as the potential for regulatory actions against your company.
- Medium-high risk: Brand engaging payments or PII use cases (Tier 1). They operate indirectly through your company's systems handling sensitive content, so they present an increased peripheral reputational risk. They engage directly with your customers so there is significant potential to harm them via financial fraud and disclosure of PII. They have limited interfaces with your systems so there is low cyber-risk. The potential for payment fraud and liability for PII disclosure present increased financial, legal, and regulatory risk.
- High risk: ISV or CSP engaging payments or PII use cases. They operate at high volume either indirectly or directly through your company's systems handling sensitive content, presenting significant reputational risk. They engage directly with your customers so there is high potential to harm them via financial fraud and disclosure of PII. They interface directly with your systems, presenting a high degree of cyber-risk. The high-volume operations produce very high financial, legal, and regulatory risk potential.

Company size and years in service can often play a role in risk assessment. A long-standing business or a globally recognized brand has a well-documented history and a reputation that can be used to develop a solid risk assessment. Fortune 500, Russel 3000, or Forbes Global 2000 companies can be counted on not to risk their global brand reputation by committing consumer fraud within Direct Carrier Billing or A2P messaging. New businesses of a few years or less have little documented history that is publicly available. Therefore, new smaller businesses are in effect an unknown entity and therefore require greater scrutiny when allowing them into high-risk ecosystems such as mobile payments.

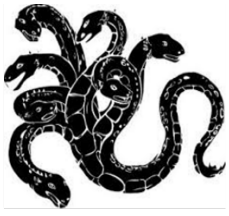
The higher the inherent risk of a partner, the more complete the diligence must be to mitigate those risks. This should not be construed as an indictment of all small and new businesses, as they can often have the potential to generate valuable new services and revenue streams. However, the unknowns associated with such businesses must be appreciated and the associated risks managed.

The discussion above introduces the importance of content and use cases in assessing risk. Beyond the obvious risks associated with more sensitive use cases involving payments and PII, certain types of use cases are likely to generate higher rates of refunds and complaints. High refund and complaint rates immediately result in increased customer care costs and the potential for regulatory attention.

Types of Bad Actors

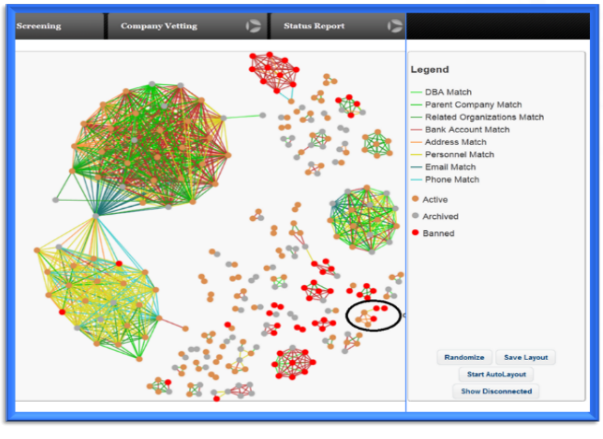
Within the telecom industry, four types of behavior have been found causing direct harm to consumers in areas of Direct Carrier Billing, Premium SMS, A2P Messaging, Location Services, Identity Services, and other value add services. Some historical use cases can shed light on the KYC best practices. Starting with relational analysis across brand partners, two fraud models have proven harmful historically. The "Hydra" model is a single entity registering multiple businesses that may be operating under an assumed or fictitious name or a legally related entity based on ownership. The fraud model is to engage in low levels of fraudulent transactions in each business across a tens or hundreds of registered business entities to ensure that anomalous transactions stay below the fraud monitoring thresholds for each business entity, but role up to substantial fraud volumes across the integrated whole. Having the relational variables within a KYC database which are tied to the registered programs can allow analytical aggregation of the individual behaviors and reveal the overall fraud behavior. From this perspective it is critically important to know that removing only one partner from your ecosystem based on bad behavior without awareness that they are still operating via other registered companies on your network will ensure their continued survival and negative experience to the customers. When performing link analysis to join entities it is important to remember that a key officer or board member of a bad actor company may also be CEO of two, three, or a hundred other business entities within your portfolio of partners. Identifying these links can help determine the true risk within your portfolio that otherwise goes unnoticed until it is too late.

"Hydra"
Same bad people operate multiple related entities
Challenge - You don't kill it by cutting off one head, you need to take down the entire operation



"Whack a Mole"
Prior fraudster returns in disguise
Challenge – Bad guys come back in a new entity or alias

A second bad actor strategy was discovered years ago when compliance organizations would identify a fraudster on a network, and act to shut them down only to have the entity reappear the following week as a new company applying for onboarding. Relational analysis and retention of an effective historical bad-actor database is the best way to prevent "Whack a Mole" behavior. The ability to link companies together by dozens of relevant variables like key employees, dba names, bank accounts, IP addresses, locations, and other parameters is critical to preventing bad actors from reentering an ecosystem as new entities.



The "Wolf in Sheep's Clothing" and "Breaking Bad" are two other categories of behavior that present unique challenges in identifying them via the verification and onboarding of partners. The nature of these players is a common tactic of laying low until trusted and then engaging in fraud actions as trust is gained for these players in the ecosystem. If a partner is new to the ecosystem, there is likely no way to know they are going to be a bad actor.

The "Wolf in Sheep's Clothing" will purposely engage in normal compliant business, become familiar with the compliance monitoring practices, and then engage in an increasing level of fraudulent actions with an attempt to maximize return while staying below the monitoring thresholds for compliance. They are smart actors who know how the entire ecosystem works and are often able to blend in as a valued partner.

"Wolf in Sheep's Clothing"
Engages in good transactions with intent to execute one (or more) fraudulent transaction(s)
Challenge – Complexity of business relationships and identifying past behaviors

"Breaking Bad"
Events occur that cause people to change financial risk-reward equation
Challenge – Monitoring and mitigating with first signs of different behaviors

The term "Breaking Bad" comes from a 2008 television drama series. It refers to a high school chemistry teacher diagnosed with inoperable lung cancer who turns to manufacturing and selling methamphetamine to secure his family's financial future. In the world of partner risk management, a bad actor may emerge for similar reasons such as a financial hardship, dislike for customers, or simply due to greed and impatience. This type of bad actor can be the most surprising as the general pattern is they did not enter the ecosystem and become a partner with the intent to commit fraud, but somewhere along the journey chose to turn to the dark side. Other variations on the theme include companies that are sold to new ownership or have turnover at the executive level positions of the company. In either case, risk has emerged that must be re-evaluated as there are general changes in principle or unknown new players leading the company.

Periodic Reverification

One thing we can count on in business is change. As a result, periodic reverification of partners is a KYP best practice. In doing so, changes in leadership, ownership, financial status, legal actions, regulatory actions, customer complaints, anomalous or fraudulent transactions, and more may all be considered in a continuously updated risk score for each partner and their programs. Some findings in the reverification process like financial hardship or relevant legal or criminal matters may be leading indicators that bad behavior could emerge. The periodic reset of partner risk scores also provides the opportunity for closer monitoring of specific partners transactions especially if you have considered customer complaints and non-compliant behavior in the re-evaluation. On the positive side, reverification also presents a path for those new and small companies that are initially assessed as risky due to unknowns to establish their trusted reputation. As such a company ages and grows while demonstrating compliant behavior its inherent risk rating improves and it rightly earns the opportunity for greater exposure in the market. In all cases, reverification is critically important in an ongoing partner risk management program.

High-Volume, Low-Cost Verification

Technology is readily available to every business, and we are seeing more companies become involved in mobile payments, large and small. The result is that a staggering number of companies may be required to be verified for a given ecosystem. How do you efficiently and effectively process the verification of tens of thousands of companies to support rapid time to market at a palatable price per unit? Verification authorities must turn to big data and automation.

For some value-add channels, the breadth of verification may warrant the use of multiple verification entities with varied expertise in the subject areas required. In other channels a simple verification that the business record on file is accurate and traceable to a real company may be enough. As result, Verification Authorities must have agile configurable platforms designed to ensure they can meet varying depths of risk analysis as required by a business channel with speed, accuracy, and a cost the market can bear. Markets also need to consider whether and how to make a participant's verification and reverification results available for use throughout the ecosystem to ensure efficient and consistent credentialing of brands across ISVs, CSPs, and Carriers.

Conclusion

The main objective of a compliance program is continuous vigilance. In their cyber security strategies, good CIOs understand that their internal systems can theoretically be hacked at any moment, so they protect all points of entry to their systems, re-evaluate those points of entry continually, and set up internal monitoring activities designed to identify anomalous behaviors.

The primary objective is to prevent being hacked with a back-up plan to shut down nefarious activities the moment they occur within their networks. The key question is when (and not if) attacked, how fast can you shut it down and how well can you protect against any loss? The answer relies on awareness of everyone on your network and an ongoing measure of their normal network activities. This allows the identification of anomalous actors or transactions to become readily apparent to network monitoring systems.

Compliance is based on the same construct: you can put many checks into the onboarding processes, but invariably the bad actors will get through and will cause harm. The role of KYC is to both stop known bad actors from gaining access to your ecosystem and to also ensure that when they do show up in your ecosystem you have the data to trace back, analyze and identify the bad behavior and shut it down at the source(s). Proper verification services up front are the building blocks of reference data that can bring clarity when bad actors begin causing harm. Furthermore, KYC is not a "one and done" practice. Periodic reverification with feedback from actual business performance of the individual partners helps the industry develop into an optimal portfolio of partners and services for its customers.

Aegis Mobile is a proud member of MEF's DCB for Growth.
Find the full white paper "Combatting Fraud in Mobile Content" developed by MEF here.