WHITE PAPER

SHINING THE LIGHT ON THE
AML/KYC BLIND SPOT
OVERVIEW

For more than two decades, financial institutions have been investing huge resources to build a robust and comprehensive Know Your Customer (KYC) program to comply with regulators and Anti-Money Laundering (AML) laws. KYC procedures enable banks to better understand their customers’ financial dealings and manage risk to their business.

Yet in our ever-growing digital age, these KYC programs still focus almost entirely on the physical, offline details of their customers, while ignoring the online presence of their customers’ identities. Almost every entity has a digital, online identity which differs from its physical one.

More traditional customers may have a minimal profile, with just an associated website and an email. Other customer profiles are almost entirely online, like e-merchants and online marketplaces. Their offline, physical identity consists only of a minimal connection to the real world.

**In today's world, is it reasonable to not understand digital risk of your customer?**

This white paper details a brief history of AML as well as the current day KYC situation for financial institutions - the fact is most KYC practices evaluate offline risk in an online world. It also demonstrates how cyber intelligence can improve your current KYC process and solution. The paper introduces an enhanced layer to your already-existing KYC procedures, known as electronic Know Your Customer (eKYC).
GETTING TO KNOW YOUR CUSTOMER

KYC guidelines are designed to help armor financial institutions from the risks of being associated with money laundering and other financial crimes. KYC procedures enable banks to better understand the identities of their customers, their financial dealings and their potential risks.

Because of their exposure to exploitation and potential fraud, financial institutions need to comply with strict and increasingly high demands, while dealing with customers who have become more complex with their digital presence and reach. Those institutions who fail to comply with these procedures can be seriously fined by regulators.

Furthermore, their AML solution must be efficient and effective, as they are handling not only regulators' demands but also those of their prospective customers. These potential customers are shopping around for speedy onboarding and account activation, which translates to minimal time to vet.

In addition to the potential accountability risk they may face if their customers engage in illegal activity, financial institutions may also lose their competitive advantage due to lengthy, complicated screening and monitoring processes.

A BRIEF HISTORY OF AML AND E-COMMERCE

Laundering money once required a great deal of effort from the criminal's standpoint. In many cases, they had to set up or purchase a brick-and-mortar business, ensure it was running legitimately, keep clean books, and incur considerable upfront operating expenses. Criminals, often drug dealers, would use this elaborate tactic to convert their dirty cash into clean dollar bills.

To combat this illegal activity and decrease crime, the U.S. adopted a set of AML regulations. Early in its implementation, U.S. AML laws were weak and largely ineffective. This changed in the 1970s, as national attention towards strict drug policy enforcement incited officials to form a regulatory enforcement organization and pass laws designed to combat laundering. Two major AML laws, which determined money laundering to be a federal crime, were passed - the Bank Secrecy Act (1970) and the Money Laundering Control Act (1986). KYC grew out of these AML regulations passed in the latter half of the 20th century, but truly came of age following the severe tightening of financial regulations post-9/11 legislation.

The U.S. government changed its focus dramatically after 9/11, shifting from illegal drugs to terrorism and counter-financing of terrorist activities. Similar to drug dealers, terrorists benefit from laundering their money, in order to fund their operations covertly. Because of the U.S. Patriot Act (2001), also known as the “International Money Laundering Abatement and Financial Anti-Terrorism Act”, financial institutions expanded their AML programs and stepped up their due diligence on foreign bank accounts.

The rest of the world also followed suit: global financial institutions invested heavily in both human and IT solutions to avoid regulatory action. AML/KYC services became a major industry and continue to grow today.
Since the 1970s, AML laws have been evolving in parallel with the Internet:

**AML Rules Brief History**
- **1970**
  - U.S. Congress passes the Bank Secrecy Act (BSA)
- **1986**
  - The Money Laundering Control Act determined ML to be a federal crime in the U.S.
- **1988**
  - Anti-Drug Abuse Act requires some businesses to report on large currency transactions
- **1992**
  - The Anti-Money Laundering Act gave birth to the Bank Secrecy Act Advisory Group (BSAAG)
- **1994**
  - ML & Financial Crimes Strategy Act creates the High Intensity ML & Related Financial Crime Area (HIFCA)
- **1998**
  - U.S. Patriot Act is born, part of it known as the International ML Abatement & Financial Anti-Terrorism Act
- **2001**
  - International Finance Corporation (IFC) launches the Global Trade Finance Program (GTFP)
- **2004**
  - International Reform & Terrorism Protection Act requires certain financial institutions to report trans-border funds
- **2005**
  - Financial Action Task Force (FATF) makes ML a crime in every state
- **2016**
  - Final Rule, to date, Published by FinCEN, AML programs include having to verify the identity of legal entity customers

**Ecommerce and Emerchant Milestones**
- **2000**
  - Chinese search engine Baidu begins
- **2001**
  - Google registers its domain name
- **2002**
  - Official launch of PayPal, originally founded 1998
- **2005**
  - Amazon.com starts selling things online; eBay founded as 'AuctionWeb'
- **2006**
  - Etsy peer to peer ecommerce website focused on handmade or vintage items and supplies starts
- **2010**
  - Public launch of Square mobile payment system
- **2016**
  - China’s Alibaba sales of products top 5463 Bn via its online shopping sites
TRANSATION LAUNDERING IS MONEY LAUNDERING

Innovation within online payments - including the surge of payment platform options, payment facilitator models, instant webstore creation technology and inexpensive hosting - has helped to make the online landscape a breeding ground for illegal activity. It is because criminals, too, are innovative in their own ways, taking advantage of the latest technologies to exploit weaknesses in the system.

In this new age, the volume of data associated with transactions is enormous, making it increasingly difficult for any player in the chain to determine the origin, target and nature of a payment and identify all the hands involved along the way. Criminals can quickly and inexpensively conceal the nature of their transactions. The evolution of e-commerce and mobile payments has essentially enabled money laundering to reach unprecedented level.

Transaction Laundering is the digital evolution of money laundering, and it has become one of the biggest challenges facing the Anti-Money Laundering (AML) regime today. Transaction Laundering occurs when an undisclosed business uses an approved merchant's payment credentials to process payments for another undisclosed store selling unknown products and services.

At the end of 2016, EverCompliant reported that $352 billion had been laundered globally through e-commerce and, of that total, nearly $11 billion involved the sale of illegal goods online. Transaction Laundering shares the same basic principles of money laundering, as it is disguising an illegal activity as a legitimate one, and can be executed on a much larger, more damaging scale.

To keep up with ever-tightening Anti-Money Laundering regulations and avoid the serious consequences of fraud, financial institutions are investing massive resources to upgrade their Know Your Customer (KYC) programs. But in the digital age, how well can existing KYC paradigms deliver on the ‘Know’ in KYC?
WHAT IS REASONABILITY IN TODAY’S WORLD?

KYC procedures for each business are built on high-level recommendations to essentially “do what is reasonable to detect suspicious activity.” However, defining reasonable has become increasingly difficult in a global banking world.

Although regulations have been in place for decades now, regulators do not always provide clear-cut requirements, leaving many pieces open to interpretation. Instead, regulators present the principle of “reasonability” – reasonable measures, reasonable suspicion, reasonable action, etc. Ultimately, it is the responsibility of the financial institutions to build and update their own policies and processes in a way that will prevent money launderers and terrorists from abusing their service and process. If a money laundering case is exposed and regulators believe that thorough, reasonably preventative actions were not taken, regulatory actions will follow.

These actions have been increasingly harsh, as evidenced in the cases against British-based Standard-Chartered and HSBC, German Deutsche Bank and Parisian BNP Paribas (BNP). The BNP case marked the first time a financial institution was convicted and sentenced for violations of U.S. economic sanctions. The judgement consisted of the “largest financial penalty ever imposed in a criminal case” at that time.
THE KYC BLUEPRINT

To understand why there is no ‘one size fit all’ model, one must first understand a financial institution's typical KYC blueprint. KYC is a key element to implementing a risk-based AML program. As KYC is connected to all other AML program elements, such as Customer Due Diligence and Transaction Monitoring, it is one of first points of contact between a customer and the AML program.

KYC is designed to assess risk levels for specific customers; i.e. how much ongoing monitoring or due diligence needs to be done. At the start of the business relationship, financial institutions request a lot of the corporate customer's information upfront, including:

- Background
- Directors and partners
- Financial situation
- Shareholder information
- Investment history
- Current and past employees

All of this information requires valid, documented evidence that is maintained in the KYC system. The collection of this data and the ability to provide this information is critical when opening a corporate account. This information varies greatly, dependent on the type of service, the type of customer, the anticipated levels of activities, etc.

No matter how a KYC program is customized, three key points are inherent to assigning a risk score to a company:

1. Countries of Operation
2. Lines of Business
3. Related Entities

PILLAR 1
COUNTRY OF OPERATION (COO)
- Where are you located?
- Where do you operate?
- Which countries do you service, are connected to, and how?

PILLAR 2
LINES OF BUSINESSES (LOB)
- What type of business or services do you have?
- What kinds of goods or services do you sell?

PILLAR 3
RELATED ENTITIES
- Who is your parent company? Subsidiaries? Branches? Board of Directors?
- What other companies and people are you connected to, and how?
We refer to these as the three pillars of AML/KYC as they are crucial to the creation of a comprehensive corporate profile. Each pillar serves as a key element in computing the AML risk score for the corporate client in any financial institution’s AML program and remains just as important through ongoing monitoring of the client.

There are key challenges to the three pillars, imposed by the realities and complexities of digital identities:

**EXAMPLE 1: COUNTRIES OF OPERATION**

The Case of Enforcing Sanction Regimes

Some of the most important policy enforcement tools of the international community are financial sanctions. Financial sanctions are implemented to enforce an international policy. They are considered to be a preferred tool over military action, and as such, compromising these sanctions can lead to serious consequences.

At EverCompliant, we investigated the case of Iran, a sanctioned country, with heavy restrictions surrounding outside business activity. We found that the number of seemingly legitimate operations with strong connections to restricted countries, including Iran, is staggering.

We analyzed a grouping of digital fingerprints, which included links to 700 sites with clear connections to Iran, including Persian text on ‘Contact Us’ pages.

These sites were selling merchandise to English-speaking websites and clearly directed at North American clients. Not only did the e-merchants advertise items for sale accepting USD, they also claimed to accept major credit cards and other payment forms, easily fooling the average user or informed financial officer, who would not dig deep into this extended network.

Take the case of a website hosted on a server located in Quebec, Canada, and with a domain registration strongly associated with Iran (company, address, phone, etc.). The website offers everything from high-resolution logos, to counterfeit and stolen goods through the sale of pharmaceuticals and nutraceuticals.

To blur the KYC lines even more, prices are denominated in British Pounds and are for very high amounts (ie: £250,000 for a Windows OS). The questions are - what is really being sold, is the money being monitored, and are the transactions in compliance with Canada’s and Great Britain’s regulations? Ultimately, what does this mean to the financial organization that authorized these corporate customers?

Even with the best of intentions and meticulous attention-to-detail, their KYC teams did not have the measures in place to suspect a thing. Unknowingly, they played a part in infringing on international laws. The failure to catch these details may have led merchants to compromise sanctions, contribute indirectly to the flow of illegal funds across countries of operations, and also potentially engage in illegal, global trade.
The e-commerce industry has been using Merchant Category Codes (MCCs) for years to effectively classify merchants and their payments processing, based on their type of business and the type of services and goods they offer. Knowing the MCC of clients is how the payments industry assigns the line of business to their customers and organizes risk. This is a basic KYC practice, as well as a business requirement, for any merchant services provider.

In the brick-and-mortar world, it is difficult to separate the merchandise from the financial transaction. If drugs or weapons were sold in a physical store, it would not be easy to make the purchase in one store, but simultaneously swipe the card in another seemingly innocent store, like a flower shop, to disguise the illegal goods. In the world of online and mobile commerce, with Card Not Present (CNP) payment methods, such separation is extremely easy to do via Transaction Laundering.

It is also much easier to promote the sales of illegal merchandise online, hidden under the legitimate and authorized e-merchants, whose lines of business may be shoes, toys or laundry detergent.

Weapons can be sold openly online, yet concealed behind layers upon layers of websites that seem unrelated to the legitimate and original MCC.

At EverCompliant, we are constantly monitoring the merchant portfolios of some of the largest global brands. A recent analysis found that 13.2% of merchants in high-risk portfolios misreported their MCC code, meaning they conducted commercial activity that did not match their registered MCC. Their true line of business was either incorrect, falsely reported or changed over time.

It is important to note that our analysis focused only on high-risk merchants. Typically, in Transaction Laundering cases, the motivation is to report a low-risk MCC (ie: book store) rather than a high-risk one (ie: casino), to bypass the inevitable scrutiny that comes with a high-risk status. Based on this analysis, it can be reasonably assumed that in assessing the entire portfolio of risk levels, the number of MCC mismatches could be much larger.

Exposing violations in content and MCC mismatches is not just about brand protection; it is also about properly identifying the types of website visitors, content and international channels to prevent scams and cybercrime. Identifying legitimate e-merchants is key for smooth business operations, with no fines or brand damage.
EXAMPLE 3: RELATED ENTITIES

High-Risk Customer Hides Network of Unreported Website Through One Reported Site

At EverCompliant, we revealed an interesting story about a seemingly legitimate merchant who sold cell phones through a domain registered with a major credit card brand. Through our analysis, we discovered nearly 4,000 connecting sites, but just one was legally registered.

The other thousands of sites were in the nutraceutical and pharmaceutical industries, foreign exchange, and many more high-risk fields.

Checking registration emails, phone numbers and other common identifiers exposed hundreds of payment pages and other indicators proving the sites were all controlled by the same, single entity.

Out of 3,999 unregistered sites, 1,184 sites were active, including 791 payment pages. These sites all contained content violations, among other violations.

Since no physical, offline KYC check showed any connection to other sites, names or countries, the ‘cellphone guy’ used his ‘phone’ sites to advertise content of illegal or controversial natures and sell his services through the various websites.

Advanced cyber intelligence would have alerted the banks that this is a high-risk customer, and prompted initial investigations, avoiding fines, fees and potential brand damage.

Mr. Cellphone’s e-Store Empire

- Number of Unregistered Websites
- Number of Active Sites
- Number of Payment Pages
THE AML BLIND SPOT: EVALUATING OFFLINE RISK IN AN ONLINE WORLD

Current KYC processes were not originally designed or updated to account for our collective shift to online identities. AML teams are using software for Customer Identification Program (CIP), ID validation, account opening workflows, data gathering forms, risk formulas and risk calculation - a variety of data validation tools, and yet, they rarely consider the vast amount of additional data that can be found online and linked to customers.

A digital identity can be vastly different from traditional concepts of a physical one. An entity’s digital identity comprises of domain registrations, email addresses, URLs, social media footprint, content and images, payment page functionality, personal and corporate names, and much more. According to research from Smallbusiness.com, 92% of small businesses will have an online presence by the end of 2018.¹

Statista predicted that by the end of 2018, 39% of all U.S. retail e-commerce is expected to be generated via m-commerce (mobile commerce).² The same source estimates that m-commerce revenue in the U.S. is expected to rise to $204.6 billion, up from $56.67 billion in 2014. According to Business Intelligence, mobile payments are expected to make a leap to $808 billion by 2019.³

It is much easier to change a hosting server than a physical office location and even easier to change an online profile in a matter of seconds. To further complicate matters, money laundering and/or terrorist funding often begins a long time after accounts have been approved; a thoughtfully-planned scheme with a strategic timeline. AML professionals need to implement periodic and accurate monitoring so that anomalous activity is detected and analyzed before it intensifies. A seemingly low-risk customer may pose a greater threat than expected, due to its network of related entities.

In today’s world, the only effective way to have a full customer profile and close those gaps involves deep analysis of the online fingerprints entities leave behind:

- What other sites are hosted on the same server or email server?
- Are other websites sharing the same phone numbers and addresses?
- Who are the companies behind these addresses?
- Are there any individuals mentioned on the website that were not mentioned in the KYC questionnaire?
- Are they related to other companies?

**ELECTRONIC KYC**

- Detects data using self-mined cyber intelligence technology
- Collects online info and enriches the existing profile
- Automatic, which can help prevent costly onboarding procedures
- Global in essence

**CURRENT KYC**

- Examine data the clients provide
- Collects and validates documents and records
- Gives AML officers a limited view of true identity
- Local in nature
ONLINE PROBLEMS REQUIRE ONLINE SOLUTIONS

As mentioned earlier, the development of AML rules and regulations does not connect directly to the evolution of the internet, social profiles and e-commerce. Financial institutions face increasing regulatory demands and massive penalties for non-compliance, and yet KYC regimes continue an offline search for risk in a world that has both offline and online details. To close the gap, KYC programs must accept the online aspects of an identity so that AML and e-commerce worlds can finally intersect and advance together.

**EverCompliant’s eKYC Discovery™** is a new, revolutionary API-driven product with the capability to look beyond a corporate customer’s physical presence to uncover unknown, online details and create a thorough business profile. This data query tool is not a replacement, but an enhancement for each step of the existing KYC process. **eKYC Discovery™** analyzes the entire Internet for risky business connections of corporate customers - including high-risk relationships to other businesses, boards of directors and source of funds - to further substantiate their identities as a legitimate business. The technology was built to leverage existing KYC investments and infrastructure to keep operations running smoothly, and to help financial institutions prevent fines, regulatory action, and brand damage associated with fraud. **EverCompliant’s eKYC Discovery™** is the cyber intelligence discovery tool of the 21st century, validating offline details with online data enabling financial institutions to make the most informed business decisions.

WHERE eKYC FITS IN AN EXISTING KYC PROCESS

- **Customer Identification Program** - Data collection and validation is vastly improved through the online verification process of eKYC. This is useful especially for smaller companies in exotic countries whose offline details may not be reliable or up-to-date.

- **Risk Screening/Traditional KYC Checks** - eKYC extends data coverage beyond the physical world to achieve a comprehensive customer profile and fill gaps of information.

- **Enhanced Due Diligence** - Automation through eKYC significantly cuts down investigation times, while greatly improving confidence in risk assessment.

- **Financial Investigation Unit** - eKYC mines more data for suspicious cases to get a full view of an organization’s entire ecosystem.
ABOUT EVERCOMPLIANT

EverCompliant is a payments industry leader in AML & KYC specializing in online cyber intelligence. Our flagship product, MerchantView™, is the first and only dedicated solution on the market designed from its core to detect and prevent Transaction Laundering. Our proprietary AI technology empowers our customers to make informed, risk-based decisions that contribute to a safer business ecosystem. We operate globally, trusted by large-scale financial institutions and payment service providers. Our headquarters is in New York with offices in San Francisco, Shanghai and Tel Aviv.

Contact us for more information or to request a free analysis of your customer portfolio: sales@evercompliant.com or visit www.evercompliant.com

U.S.
85 Broad Street, 18th FL
New York, NY 10004, USA
P: +1.646.665.4331

Israel
55a Yigal Alon St
Tel Aviv 6789153, Israel
P: +972.3.652.4747