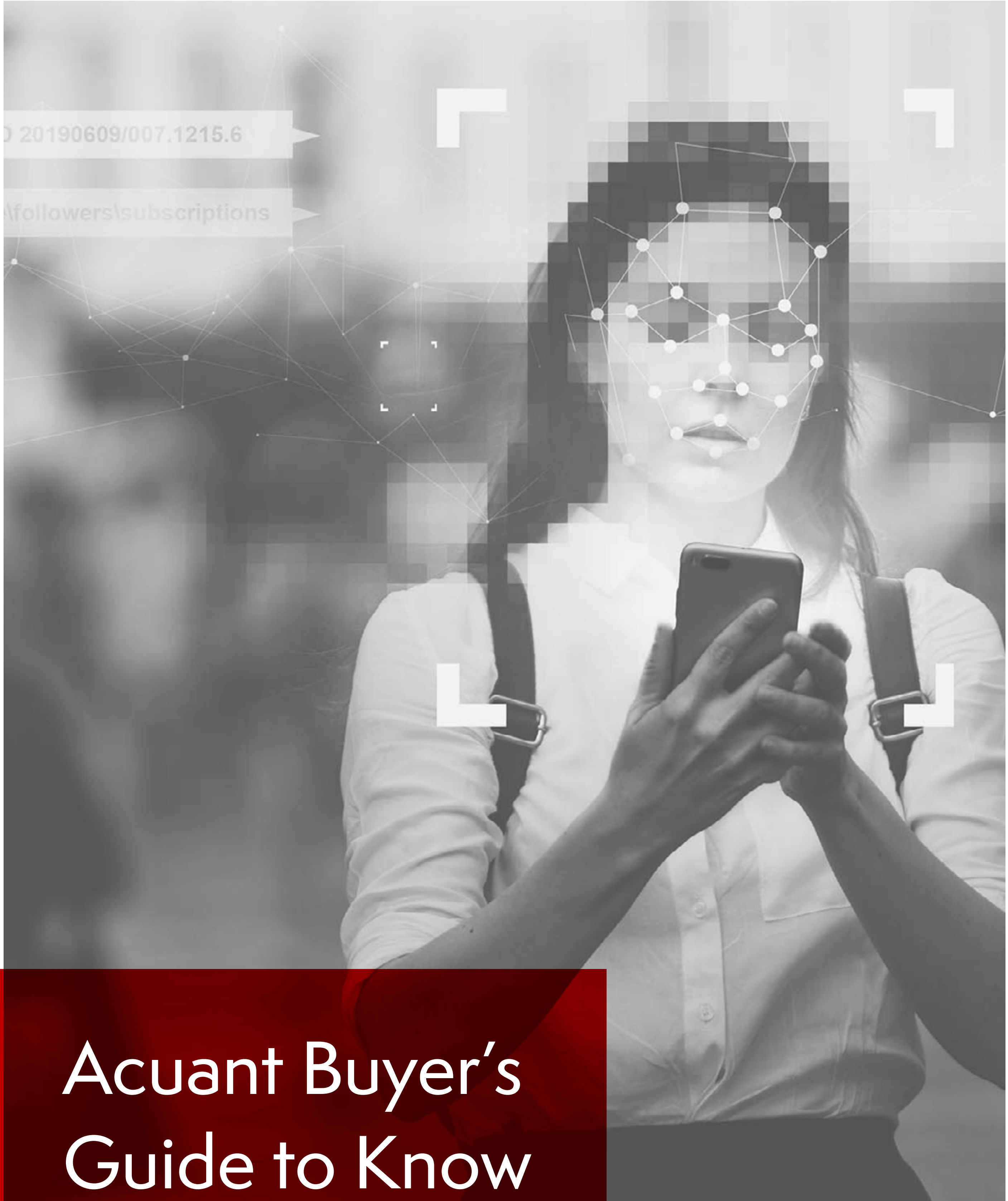
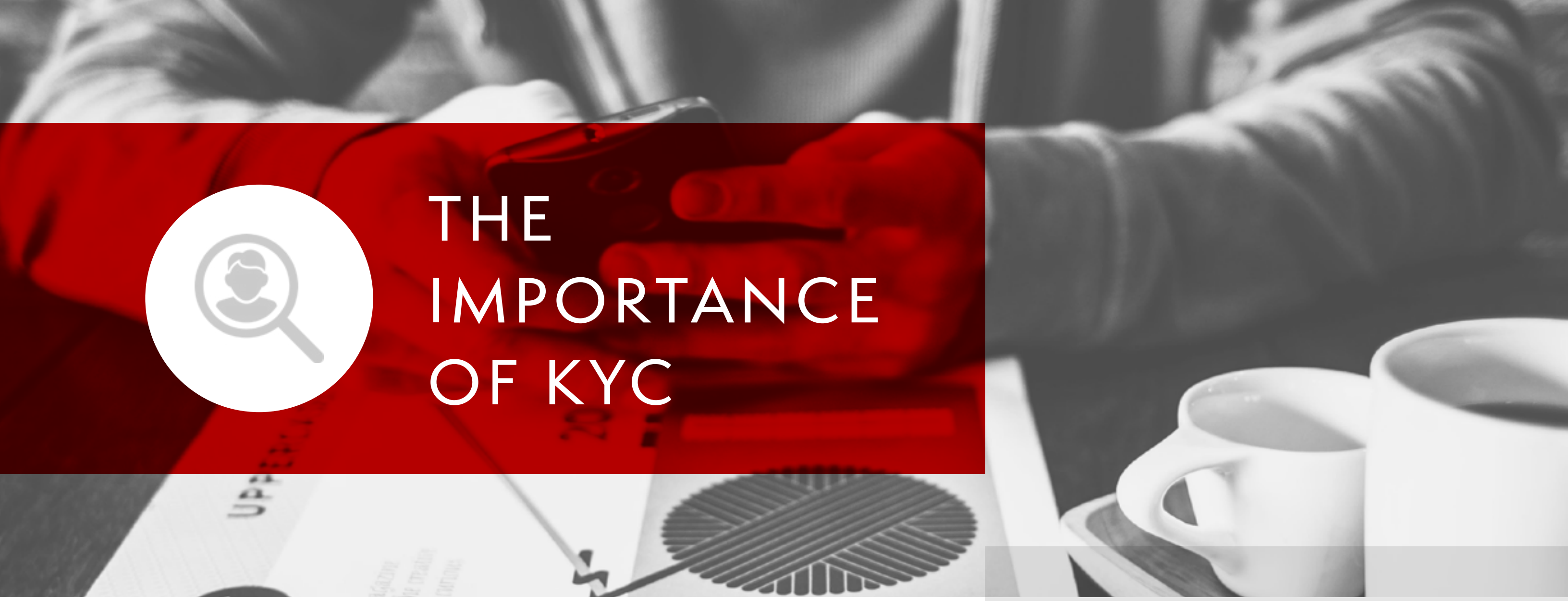


Acuant Buyer's Guide to Know Your Customer

acuant
a GBG company



THE IMPORTANCE OF KYC

Building a business can be challenging in today's digital world where fraud seems to come from every direction. Establishing trust goes both ways – customers want safe transactions and companies want to make sure they are transacting with good customers. It is important to verify that your customer is who they say they are and that you can trust them. Equally, you want them to trust your business. For regulated businesses, this is a requirement called Know Your Customer (KYC) and it is a subset of Anti-Money Laundering (AML).

KYC is a key part of Anti-Money Laundering regulations. Introduced as part of the Patriot Act, KYC requires that financial institutions identify and verify customers to ensure they understand who their customers are and the level of risk they pose. The goal of the regulation is to minimize money laundering and related fraud. It's estimated that up to $2 trillion USD is laundered globally every year and in response, AML regulations have expanded around the world. Recent examples include the Anti-Money Laundering Act of 2020 in the US and 6AMLD in the EU. Failure to comply with AML regulations has resulted in steep six and seven figure fines. In the US, institutions must report the origins of sums exceeding $10,000 as well as monitor and report suspicious activity. Mandates vary around the world.

WHAT IS THE DIFFERENCE BETWEEN AML & KYC?

Anti-Money Laundering (AML) refers to a wide set of laws and regulations designed to prevent money laundering, terrorist financing and to stop criminals from disguising illegally obtained funds. Financial institutions must not aid in money laundering, either knowingly or unknowingly.

Know Your Customer (KYC) is a component of AML that consists of firms verifying their customers' identities, either before or during the time of their transactions, and is a key part of any organization's AML compliance program.

KYC consists of 3 Pillars:

- Customer Identification Program (CIP)
- Customer Due Diligence (CDD)
- Continuous Monitoring

WHO MUST COMPLY WITH KYC

Because KYC is part of AML, the main industries that must comply with these regulations are in the financial sector. KYC compliance, however, continues to expand wherever money laundering may be a concern. Retailers, for example, may be subject to KYC regulations as more eCommerce and peer-to-peer platforms are designated as Money Services Businesses (MSBs) and are becoming targets of fraudsters.

The types of business that must comply with KYC varies between jurisdictions. In nearly all countries the regulated sector includes:

- **Banks and Credit Institutions**
- **Stock Exchanges and FX Dealers**
- **Money Services Businesses**
- **Asset Managers**
- **Company and Trust Formation Services**

In some jurisdictions the regulated sector has expanded to include:

- **Accountants, Auditors and Tax Advisors**
- **Legal Professionals**
- **Bookmakers and Casinos**
- **Estate Agents**
- **Insolvency Practitioners**
- **High Value Goods Dealers Involving Cash Payments**

It's important to note that while KYC is a compliance requirement for businesses in regulated industries, knowing your customer and determining risk is, in fact, a best practice for any business in any industry looking to transact and interact with trust and confidence. Wider enforcement of expanding regulations means any business looking to scale globally should be concerned about KYC. Another major factor to adopting KYC processes is if your integrations mandate it – the financial or payments platforms that your business uses will often require thorough KYC.

COMPLYING WITH EXPANDING REGULATIONS

In the US – FinCEN is the regulator that interprets and enforces the regulations designed to combat money laundering and terrorism financing. Laws include BSA, PATRIOT Act and the Anti-Money Laundering Act of 2020.

Other internationally notable AML laws and regulations include TACT & POCA (UK), 6AMLD (EU), Anti-Money Laundering Law & Anti-Fuel Theft (Mexico)

International AML Regulators include:

- Financial Action Task Force (FATF) with over 200 FIUs that follow the 97 FATF recommendations
- Comisión Nacional Bancaria y de Valores (CNBV) – Mexico
- Anti-Money Laundering Authority (AMLA) – EU
- Financial Conduct Authority (FCA) – UK
- Financial Transactions and Reports Analysis Centre (FINTRAC) – Canada
- China Banking and Insurance Regulatory Commission (CBIRC) – China
- Hong Kong Money Authority (HKMA) – Hong Kong
- Australian Transaction Reports and Analysis Centre (AUSTRAC) – Australia

And many others that give recommendations and enforce regulations

Establishing a Trust Framework Via Secure Onboarding with Acuant

While KYC is imperative for financial institutions, any business can benefit from verifying its customers. Establishing a good, trusted relationship with your customers starts during the onboarding process. Trusting your customers means, in part, that you know who they are and that you believe that working with them does not represent a significant risk to your business.

Acuant has developed a patent-pending Trust Framework that answers the four most important questions to establish a trusted relationship with your customers.

QUESTION 1: **IS THIS A REAL PERSON?**

First and foremost, when interacting and transacting with your customers, it is important that you do so with real people. There are a number of tests that can be performed to verify the validity of the provided identity data.

Document Verification: Capture information from government-issued identity documents and authenticate the document. Global coverage is important for accurate document and identity verification and complying with the most up-to-date KYC regulations.

Acuant has the largest library of government-issued documents from around the world that is continually being updated for latest versions and reading new security features. Read why document onboarding velocity is crucial for identity verification in the white paper **Guide to Adopting Identity Verification**.

Data-Centric Validation: Checking identity data against global databases such as credit agencies, utility bills, change of address, voter registrations and property ownership records helps to establish that person has made other transactions. Dark web searches can also help determine whether the identity has been created from stolen information or compromised data.

Combining document verification with data-centric validation is an important first step to evaluating the risk of onboarding a new customer. Acuant automates seamless access to global databases to verify customer information in seconds. Capture ID document data with accuracy, authenticate documents with the industry's largest document library and verify information with data-driven verification through credit agency, database and alternative data sources such as social media and the dark web.

QUESTION 2: **IS THIS PERSON WHO THEY CLAIM TO BE?**

Once you have verified that the data provided to you is valid and associated with an actual identity, the next step is to confirm that the data matches with the identification provided and the device used during the customer onboarding process by that same individual.

Facial Recognition Matching and Liveness Tests: Match the photo on the ID to the person claiming it, to ensure they are present during onboarding and to validate against identity attributes previously provided.

Facial matching technology and liveness must be spoof-proof to ensure a video or photograph is not being presented in place of a real person. The type of face match and liveness chosen matters in the customer experience as well. Asking customers to take time to smile, blink or make gestures can create unnecessary friction in the onboarding process. Acuant's platform has user-friendly face matching and liveness with options for passive liveness where no additional movements are needed. Fraudsters also will not be cued that the liveness test is happening. Acuant utilizes Passive Liveness which meets Presentation Attack Detection (PAD) Level 1 and 2 and has been extensively tested against photo substitution, video replay and masks.

Device Analysis, Geo-fencing and Geolocation: Verify that the location of the device being used is consistent with other data collected and confirm the device is not associated with multiple accounts or suspicious transactions.

Acuant offers a variety of verification methods which can be applied depending on level of scrutiny. A large set of verification runs in the background, which reduces friction for the customer.

QUESTION 3: **CAN I DO BUSINESS WITH THIS PERSON?**

When the provided identity data is validated and connected to an actual identity, the next step is to determine whether or not you will be able to transact with that individual. Doing so is essential for regulatory compliance and to avoid transacting with high-risk persons and entities. This is determined by screening customers against global sanctions and PEP (Politically Exposed Persons) lists that identify individuals engaging in illegal activities.

Acuant's Sanctions Screening capabilities leverage over 300 sanctions and PEP lists including:

- Office of Foreign Assets Control (OFAC)
- Interpol
- EU Consolidated List of Sanctions
- UN Sanctions List

Acuant Sanctions Screening uses a wide array of algorithms to decrease false positives and the flood of alerts that follow, while making sure your business is following AML regulations. The platform also enables custom lists and alerts based on risk profiles.

QUESTION 4: **SHOULD I DO BUSINESS WITH THIS PERSON?**

After the first three questions are confidently answered and verified, it's essential to continue evaluating the risk to your business when transacting with your customers.

This is best done using machine learning and graph intelligence to monitor transactions and user behavior. Machine learning is key for understanding risk and using continuous data inputs with risk scoring engines to flag untrustworthy behavior. Graph intelligence will help you evaluate the relationships between users and other entities to determine the level of risk to your business if you choose to transact with them.

Digital Identities and Identity Risk Scoring: Acuant's platform protects your organization with dynamic identity risk scoring, going beyond a fixed set of rules to flag suspicious behavior. The wealth of data can be integrated into Acuant's patented eDNA® engine which combines graph intelligence and machine learning to evaluate customer data and the connection between other customers which can then uncover associations with untrusted entities. For example, multiple people sharing a payment method or address might be a family or a fraud ring.

Transaction Monitoring: Create alerts for suspicious behavior and track transactions. This may include having adverse media checks which flag names and companies that are reported in the media and other sources. A customer with a bad reputation puts your business at risk.

Always remember, even if a customer was identified as trustworthy during onboarding, that may not be true for future transactions. The risk profile of your customers will change over time based on their most recent interactions, changing financial circumstances or compromised credentials or accounts. Companies that take a periodic testing approach to trust and identity do not assume that their customers' situation has remained the same.

CHOOSING A KYC PROVIDER

KYC compliance requires three levels of due diligence with increasing scrutiny between each level. Verifying a customer during onboarding and re-verifying throughout the customer journey based on their behaviors in your business ecosystem protects from account takeover or muling where months may pass before a fraudster makes a move.

LEVELS OF DUE DILIGENCE FOR KYC

Simple Due Diligence (SDD) is used in situations where the risk of money laundering or terrorist funding is low. For example, in accounts with low transaction values and volumes, the opportunity to perform illegal activity is limited. Therefore, these small value accounts can be exempt from stringent due diligence to help reduce onboarding friction for customers and financial institutions.

Customer Due Diligence (CDD) is information obtained on customers to verify their identity and assess the risks associated with that customer. These are the checks most typically taken out on customers when opening a financial account in some form.

Enhanced Due Diligence (EDD) is additional information collected on higher-risk customers to provide a deeper understanding of activity to mitigate associated risks. For example, most jurisdictions require politically exposed persons (PEPs) to go through the EDD process. Other factors that might trigger EDD are high value and volume accounts, accounts that deal with high-risk countries or accounts that deal with high-risk activities.

Your business may have ranges of low to high transactions as well as volumes that are too large for compliance officers to manually review. A KYC solution with a risk-based approach will reduce friction for lower risk transactions and scale appropriately.

The Acuant platform is designed to evaluate the possible associated risk of account information at the time of onboarding and/or transaction with true dynamic risk assessment. This is done using a risk matrix - two evaluation engines “AML Profiles” and “Fraud Profiles” combined with different risk profiles can be pre-configured to determine levels of scrutiny to be applied during the application process. Good customers are passed through faster, and additional due diligence can be added depending on the transaction threshold or for suspicious profiles.

AUTOMATION TO REDUCE FRICTION

A manual KYC process simply does not cut it today. Businesses must keep up with customers, sophisticated fraudsters and growing compliance costs. A manual process is not only expensive in that you must hire and train teams to maintain it, but it can also lead to fines, business stoppages, losses related to fraud and customers leaving. Implementing a system that is cost effective and drives an efficient KYC/AML program is a must.

Automation is a great way to keep up with the speed of the digital world, however, speed alone is not going to make a flawed process more effective. Accuracy is equally critical. A KYC system that uses machine learning to build identities that accurately reflect the level of risk that they pose will reduce errors. No one wants a flood of notifications and a system that triggers excessive false positive alerts because customers or prospects have a common name.

If your compliance system generates a lot of false positives (or negatives) your team will be flooded by notifications that can hinder their effectiveness and turn away good customers. If your compliance system uses a static approach to risk, then it may include too much friction for your good prospects, effectively turning them away. If your compliance system does not provide accurate and tunable risk thresholds, then it may not match your risk tolerance and will be unable to identify the riskiest prospects, or will add unnecessary friction for good, trusted customers.

The right KYC system fits into your compliance operation in two ways

- ✓ It easily integrates with your current systems
- ✓ It aligns well with your current processes

A major factor to avoid when implementing a new solution is disruption to current systems. An open and easily deployed solution will facilitate a more streamlined integration without wreaking havoc on your IT environment.

If a compliance system does not fit in with your other technologies, it will not be able to improve your process or results. This means you need a system with a breadth of features that can be deployed as modules that fit your current and future needs. It's best to ensure easy access and integration with a standards-based API.

Be prepared for the likelihood that your processes will not change on day one. It will be a transition, so ensure that analyst tools like dashboards and case management are configurable and include the information and capabilities your team needs to be successful. Reports and rules should also be easy to configure and not require a consulting engagement to change. Additionally, the solution should offer coverage and capabilities for all the jurisdictions where your firm operates.

EFFICIENCY		IMPLEMENTATION
Operations (operate faster)	Analytics (operate smarter)	Deploy + Configure
▪ Automated Decisioning ▪ Rules-Based Routing • Rules engine customized by industry, business model and regulatory requirements ▪ Case Management ▪ Queue Management ▪ Pre-Populated SAR Filing	▪ Digital Identities ▪ Machine Learning-Based Risk Scoring ▪ Risk-Based Approach ▪ Dashboard ▪ Notifications ▪ Reporting	▪ Standards-Based API for Easy Integration ▪ Configurable Agent View ▪ Visual Administrator Tools for Rules, Sanctions and Integration Configurability ▪ SDK ▪ Pre-Integrated with Verification Vendors

NEVER FORGET THE CUSTOMER EXPERIENCE

Customer experience is vital to engaging prospects, turning them into customers and keeping them. The right KYC system will not only safeguard your onboarding experience but provide a strong and engaging experience for your customers. This means that the right system does not force you to sacrifice security for a better customer experience. Effective automation, a risk-based approach and machine learning are important technology components to help you turn the dial up on better security without compromising on experience.

ONE PLATFORM FOR END-TO-END KYC & AML COMPLIANCE

Acuant's Trusted Identity Platform provides end-to-end KYC and comprehensive AML compliance that is cost effective, secure and enhances operational efficiency. The platform facilitates the implementation of cost-effective AML and risk strategies for a risk-based approach at different levels. Businesses develop models to classify the risk associated with their clients and can then implement policies and processes accordingly to evaluate users. Advanced AI technology allows you to automatically approve or deny prospects, operational technologies make your compliance team more efficient and digital identity technology helps you understand the risk of a specific identity and enables you to react in real time. Fit your current systems and needs with our API access, modular approach and custom capabilities. Our risk-based approach applies additional due diligence to suspicious users while showing trusted users the fast lane.

Acuant US

–

Los Angeles, CA
Manchester, NH
Palo Alto, CA
Spokane, WA

Acuant EMEA

–

Brussels, BE
Manchester, UK
Tel Aviv, IL

Acuant LATAM

–

Mexico City, MX

Contact Us

–

info@acuant.com
acuant.com