PRIVITAR

Anti-Money Laundering and Anti-Fraud

A Rapidly Evolving AML Landscape in the Digital Age

Banks worldwide spend over $8 billion[1] annually for anti-money laundering (AML) compliance and additionally spend $321 billion[2] in fines for being in violation of a range of issues related to AML and fraud. The UN Office on Drugs and Crime estimated the global amount of money laundered per year to be between $800 billion and $2 trillion in 2019, or 2-5% of global GDP.

In the digital age, criminals have evolved to stay one step ahead of banks by exploiting the volume of transactions, deploying ransomware[3], and benefiting from multiple data sources that organizations must track in parallel. Increased digitization means financial institutions have to move even faster to track, cross-reference and report on suspicious activity.

The threat of organizations not detecting AML activity is ever-present, and the negative impact to their customers, brand image and integrity of business processes are high. As if these issues were not enough, there is also the persistent requirement to remain compliant with government legislation such as the Bank Secrecy Act (BSA). These sets of regulatory directives are destined to increase in complexity, particularly for global institutions. Some of these regulatory requirements are even seen as being "diametrically opposed"[4], such as the Right to be Forgotten via GDPR and CCPA conflicting with the requirements around Know Your Customer (KYC) reporting and crime prevention.

Given these factors, what is the best way to stay compliant without risking too much data being accessible? How can financial institutions ensure they're following regulations while maintaining their customers' privacy and their brand's integrity?

Automation and Data Privacy: The Future of AML

The BSA, among many other global regulations, requires several checkpoints and processes to ensure effective procedures. Central to these requirements is identifying who the involved parties are in each set of transactions to scan against many different lists of suspicious persons and understanding the relationships between the parties involved. This requires a significant amount of sensitive data to be in and out of the hands of data analysts, as well as a location where the data can be tracked and maintained. The volume of transactions, as well as the disparate lists and other sources of information to verify against often require huge amounts of data to be stored safely and securely. In this case, "safe and secure" not only means standard requirements around IT infrastructure, but also who has access to the data, for what purpose, and how much of the raw data each individual can see.

1. Forbes.com, 2019.
2. Payments: Cards and Mobile, 2018.
3. Fico.com "5 Reasons Why AML is More Important than Ever in 2019". 2019.
4. Payments Cards and Mobile, 2018.

Risks related to data integrity do not come from external sources alone; IBM reported in 2019 that 60% of data breaches were due to insider threats or negligence. With this high level of risk it is crucial to provide the ability to provide data privacy to sensitive data in the hands of analysts, while also maintaining referential integrity to enable those analysts to do their jobs effectively.

Even with this referential integrity and safeguarding against risk, this is a time-intensive and granular process that requires significant resources to support; increasingly, enterprises are extending processes to include third parties in automation of their AML activities. Automation historically saves companies time and resources, which can then be devoted to more complex analyses, but it also opens up new risks. Within this extended structure, institutions must not only comply with BSA, KYC, GDPR, CCPA and many other regulations; they must also deliver regular, transparent and robust reporting proving such.

Ensuring that customers can be forgotten and their privacy protected is paramount, and equally important is the need to prevent fraudulent activities. Traditional security measures, such as firewalls, encryption, and access control, are no longer enough. Privacy must go hand in hand with AML activities to adapt to the increasingly demanding requirements.

Layering Data Privacy on Top of Existing Security

A simple use case might be that a financial institution currently has a staff working full time on AML activities – checking against terrorist watch lists, other flagged or suspicious activity, and cross-referencing relationships between parties in each transaction. Data must be de-identified to protect the privacy of the individuals who have not been engaging in fraudulent activity, and must be tracked to ensure both what systems the data is being managed on and in what jurisdiction it is being used in. Many enterprises are also looking to introduce automation of these activities via third parties, introducing more complexity; control must be extended to ensure data privacy includes any and all outsourced parties in the AML process. This complex infrastructure requires tracking and data management via:

- Privacy Protection. De-identifying data mitigates risk and protects the privacy of loyal customers. It adds a layer of protection not only at rest and in transit, but also while data is in use, whether internal or 3rd party. Unlike encryption alone, which protects data at rest, data de-identification protects data in transit and in use, allowing for more flexibility in automating or offshoring AML processes.
- Controlled Linkability. Ensuring de-identified transactional data can continue to be joined with watch lists but cannot be intentionally or accidentally enriched to re-identify customers is essential. Especially so when collaborating with 3rd parties whose controls are outside your purview.
- Separation of Authority. Governmental regulations and company policies require a separation of powers. The individual who defines data governance policies must be separate from the AML analyst using that data on a regular basis to identify potential risks. Each of these must be distinct from who has the authority to apply de-identification and re-identification rules to the data.
- Centralized Control. A centrally managed, intuitive way to define Policies and Roles and to systematically enforce them maximizes productivity and adherence to regulations and policies.
- Dataset Tracking. Datasets must be uniquely identifiable to afford full traceability. This includes information on when the dataset was generated, who can use it, how it will be used and when it should be deleted. This facilitates demonstrating compliance with corporate policies and government regulations. And in the event of a breach, accelerates forensic investigation and required notifications.

The Privitar Data Privacy Platform: Helping Organizations Achieve Success

Security alone is no longer enough to ensure that competing demands of AML/anti-fraud, privacy regulations, corporate policies and brand value are all being achieved. Privitar supports the demanding requirements of AML/anti-fraud analyses and investigations while respecting customer privacy.

> De-identification: Privitar provides the full range of techniques to preserve data privacy holistically. While encryption can secure data in transit and at rest, de-identification goes a step further to ensure that even when in use, data is protected. Privitar supports redaction, reversible tokenization, generalization and perturbation among other techniques to preserve customer privacy throughout the AML process, even during analysis.

> Central Policies: The Privitar Platform enables Privacy Policies to be defined centrally and applied either systematically or by privileged users. This design ensures Policies are applied consistently across all environments, allowing enterprises to set once and be assured of protection of their valuable customer data.

> Watermarks: Privitar Watermarks are unique technology that enable end-to-end traceability of sensitive data. Watermarks allow tracking and management of when the data was generated, who it was generated for, when it should be deleted and where it will be used.

> Separate Roles: Providing separate roles for who can see and use data ensures even more control over processes related to AML activities and compliance with regulations like the BSA. Key roles provided in the Platform are:

Administrator: Manage the environments included in the Platform.

Author: Create, edit and delete Privacy Policies, Schemas and safe datasets, which we call Protected Data Domains™.

Operator: Run jobs to de-identify data.

Investigator: The only role that can investigate and trace the origin of the data.

Unmasker: Run jobs to re-identify specified de-identified data that was originally defined by the Author to be reversible.

With the Privitar Data Privacy Platform enterprises can make the most of their data in light of increasing regulations and still leverage automation that allows them to employ efficiencies to their AML process. Adding Privitar to the AML/anti-fraud procedures within an organization will benefit both the automation process, and AML management itself.

Contact us:

e: info@privitar.com
t: UK +44 203 282 7136
US +1 857 347 4456
w: www.privitar.com

PRIVITAR

@PrivitarGlobal

www.privitar.com