1 **OVERVIEW**

2 **CHALLENGES**

3 **THE OPAQUE SOLUTION**

4 **OPAQUE ADVANTAGES AND KEY CAPABILITIES**

Financial Services
Advancing AML Compliance

OVERVIEW

Financial institutions are required to follow specific procedures to prevent criminals from using their platforms to disguise the origins of illegally obtained funds. The process of detecting and preventing money laundering is difficult, with criminals going to great lengths to disguise transactions and move data across various banks and geographies.

Opaque empowers AML by allowing financial institutions to collaborate and analyze information while ensuring privacy. With Opaque, banks can securely share data sets without exposing sensitive information. This allows for patterns of criminal activity to be identified more easily.

CHALLENGES

Detecting money laundering requires the ability to effectively process large data sets from multiple sources. The solution not only needs to enable advanced analytics and model training, it needs to preserve the confidentiality of the underlying data. These data sources often contain confidential personal information and the data cannot easily be shared.

It's not simply a matter of masking the personal information and proceeding with analytics. When personal information is masked, it becomes difficult, if not impossible, to identify the relationships between different entities, such as customers and bank accounts. Without the ability to identify these relationships, financial institutions find it extremely difficult to identify patterns of money laundering, even though money laundering costs governments and businesses billions of dollars every year. In an effort to crack down on money launderers, many countries have implemented stringent anti-money laundering (AML) compliance regulations. However, complying with these regulations can be difficult, especially when it comes to identifying suspicious activity.

The first step in any AML compliance program is to identify suspicious activity. This can be a difficult task, as money launderers are often very sophisticated and use a variety of methods to conceal their activities, including:

- Splitting transactions into multiple smaller transactions in order to avoid detection.
- Using different bank accounts in different countries.
- Sending money through intermediaries or shell companies.

THE OPAQUE SOLUTION

The Opaque Confidential AI and Analytics Platform provides a powerful solution to ensure compliance and prevent financial crimes. The Opaque Platform allows financial institutions the ability to collaborate and analyze information while ensuring privacy and protecting sensitive information.

Opaque addresses AML compliance by providing confidential artificial intelligence (AI) and analytics solutions that help organizations identify suspicious activity. By sharing information, banks are able to identify larger patterns of criminal activity and more effectively identify money laundering – without violating privacy laws and compliance regulations.
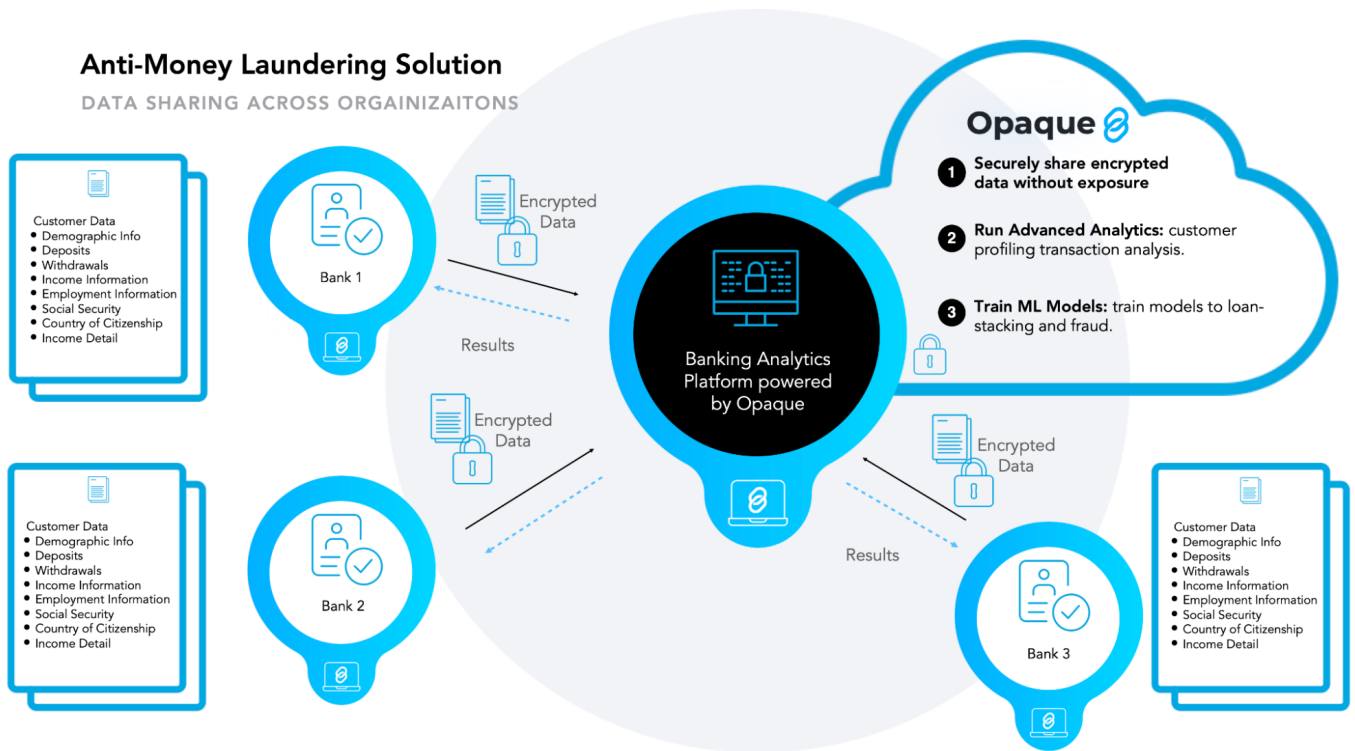
Financial institutions must carefully weigh the benefits of sharing information against the risks of violating privacy laws and/or incurring fines from regulatory bodies. On the one hand, financial institutions need to analyze large amounts of data in order to identify suspicious activity. On the other hand, financial institutions are required to protect the privacy of their customers – many financial institutions are reluctant to share information with other organizations for fear that their data will be misused or stolen.

Opaque allows financial service institutions to perform analytics, train and run AI models at scale on encrypted data, and collaborate securely within and across organizational boundaries. With the Opaque platform, organizations can establish confidential collaborative workspaces across multiple teams and combine encrypted data sets without exposing data across team boundaries.

Multiple banks can collaborate to more effectively identify suspicious activities with fully encrypted data. With Confidential AI and Analytics, banks can perform entity resolution accessing the encrypted data across each bank and track transaction patterns to more easily identify money laundering activities.
The Opaque Confidential AI and Analytics Platform provides a powerful cloud-based solution powered by hardware-based Trusted Execution Environment (TEEs). With Opaque, data is encrypted at rest and in transit, and is protected while in use. Any data in the TEE can't be accessed or tampered with by any code outside that envi-

The Opaque Solution

Anti-Money Laundering Solution
DATA SHARING ACROSS ORGAINIZAITONS

Opaque

1. **Securely share encrypted data without exposure**
2. **Run Advanced Analytics:** customer profiling transaction analysis.
3. **Train ML Models:** train models to loan-stacking and fraud.

Banking Analytics Platform powered by Opaque

Customer Data
- Demographic Info
- Deposits
- Withdrawals
- Income Information
- Employment Information
- Social Security
- Country of Citizenship
- Income Detail

Bank 1

Bank 2

Bank 3

Encrypted Data

Results

---

① **OVERVIEW**	ronment. This approach removes the ability for a cloud provider or other actors in the domain to access code and data while being executed.
② **CHALLENGES**	**OPAQUE ADVANTAGES AND KEY CAPABILITIES**
③ **THE OPAQUE SOLUTION**	**Data Protection Throughout the Lifecycle -** Opaque protects all sensitive data (e.g., PII and SHI data) using advanced encryption as well as secure hardware enclave technology, throughout the lifecycle of the analytics computation—from data upload to applying the analytics models to obtaining the results.
④ **OPAQUE ADVANTAGES AND KEY CAPABILITIES**	**Secure Computation in the Cloud -** The Opaque Platform ensures that no data is ever exposed and data in use and in transit always remains encrypted. Additionally,

(1) OVERVIEW

(2) CHALLENGES

(3) THE OPAQUE SOLUTION

(4) OPAQUE ADVANTAGES AND KEY CAPABILITIES

Opaque's Platform also guarantees data privacy, trust, and compliance during data access, data processing and analytics.

Secure Multi-Party Collaboration and Data Sharing - With Opaque, data teams benefit from combining their data together and analyzing it jointly to obtain mutually beneficial insights. The solution ensures that the data of individual owners is never exposed to either the cloud environment or to other data owners. Each data owner retains full control over how their data is used.

Secure Collaborative Analytics - Data scientists can use Opaque to do much of what one can do with Spark SQL: run rich SQL-based analytics on the data; perform statistical analysis; or manipulate data using projections, filters, joins, sorts, and aggregations. Opaque preserves the Scala, SQL, and Python APIs provided by Spark—data scientists who know SQL or have previously worked with Spark through Scala or PySpark, already know how to use Opaque.

State-of-the-art Cloud Security - Opaque maintains the security of these advanced clouds and further provides the second layer of security based on hardware enclaves and cryptographic fortification. Opaque thus makes it exceptionally difficult for attackers to attempt to subvert both security layers of Opaque. As a result, the Opaque Platform provides a very high degree of security, much stronger than the traditional security of even prominent clouds today.

Opaque's technology is widely applicable and can help address a wide range of use cases across a diverse set of industries.
For more information on use cases visit: *https://opaque.co/solutions/*