

SOLUTION BRIEF

Mergers & Acquisitions

The Background

Each year, merger and acquisition (M&A) deals worth billions of dollars are closed around the world, with the financial services and insurance (FSI) industry accounting for the highest value transactions. It's easy to understand why — M&A processes are one of the primary avenues for FSI firms to quickly scale up operations, reach, and customers. By combining operational infrastructures, capabilities, and talent, organizations that undergo an M&A are often able to fill existing gaps, increasing efficiency, competitiveness, and customer service.

However, M&A transactions can be complex and, with highly sensitive personal financial data involved, risky. In today's global economy and interconnected world, personal data is routinely collected and used, so organizations participating in an M&A must have a plan for keeping data secure throughout the process and beyond.

The Challenge

According to [Deloitte](#), one of the primary reasons M&A deals fail at a surprisingly high rate — between 70% and 90%, per [HBR](#) — is data privacy and regulatory concerns. When organizations merge with or acquire another company, business operations, the number of data users, and the scope of data use instantaneously grow. With both firms combining their own data sets, there must be an efficient way to ensure that data protection methods and standards are consistent, only authorized users are able to access data for approved uses, and privacy regulations are adhered to across jurisdictions, taking into account internal rules, industry standards, and federal laws. Once established, the organization must also be able to provide comprehensive auditing to prove compliance.

Without a strong data governance framework, stakeholder buy-in, and automated tools that work across both companies' data ecosystems, this can lead to unmanageable and risk-prone processes that inhibit the value of combined data.

The Solution

To help data teams efficiently manage data access at scale, prevent unauthorized access or leaks, and adhere to stringent regulatory and contractual guidelines during and after M&A, FSI firms need an all-in-one solution — not a collection of disparate tools. Immuta helps meet these rigorous demands using a variety of advanced techniques:

- **Attribute-Based Access Control:** Ensures access control is dynamically granted on a legitimate, as-needed basis by mapping policies to user attributes such as title, location, data source, and purpose, enabling secure access control that is easily scalable.
- **Sensitive Data Discovery:** Automatically detects, classifies, and tags sensitive data to streamline consistent policy enforcement without risk-prone manual processes, simplifying the process of aggregating both parties' data sets securely.
- **Row- and Column-Level Security:** Dynamically masks, redacts, or exposes data in specific rows or columns based on access control policies enforced at query time to help ensure sensitive personal information remains hidden.
- **Dynamic Data Masking and k-Anonymization:** Applies advanced privacy-enhancing techniques (PETs) to preserve data privacy without increasing time or risk by copying or moving data.
- **Audit Logs:** Monitor and show who accessed what data, when, and for what purposes to demonstrate compliance with regulations, contracts, and other data privacy rules.

The Outcome

FSI firms that leverage Immuta's cross-platform data security and access capabilities during an M&A experience:

1. Faster time to data access and ability to start using data to drive business outcomes as a result of streamlined data preparation processes.
2. Greater efficiency of data engineering resources in aggregating data across organizations and ensuring the right protection is consistently applied to all data.
3. Improved ability to maximize data's utility while preserving its privacy and security, resulting in higher customer service levels.
4. Transparent compliance with federal and industry regulations regarding the use of sensitive data with the ability to show information is used only for its contractual purpose.

Ready to get started?

REQUEST A DEMO

START A TRIAL

