FACT SHEET

Seven Reasons Financial Institutions Should Consider Authorization

The finance industry has the second highest average cost for a data breach, according to a recent Cost of Data Breach report. In fact, the average cost of a breach in the finance industry increased to $5.97 million in 2022. These records are so valuable because they contain private financial information of customers (both individuals and businesses of all sizes), making them sought after pieces of data.

Due to their value, all financial institutions must protect each customer's privacy and confidential information while adhering to global compliance regulations surrounding access control, segregation of duty, and the right to be forgotten. This comes with multi-pronged data access control challenges, particularly when it comes to privacy and compliance.

As a result, many financial institutions have implemented authorization solutions to solve their access control challenges. However, there is room for improvement. To that end, a recent survey by SailPoint reports that 97% of respondents agree that their organization's ability to detect and prevent identity-related security breaches needs to improve.

A critical way in which to have a more successful approach to access control that adheres to modern security standards including Zero Trust is to implement an externalized authorization solution. This solution externalizes access control decisions to a decision point that is decoupled from the application which provides data and transaction protection capabilities.

Here are seven reasons financial institutions can use authorization to solve their access control challenges.

1

1 Online payment authorization

International payment providers continually seek to reduce operational costs associated with transactions. The challenge - they must do so while also ensuring they can pass an audit.

An authorization solution can secure web services and APIs used in the payment application while also increasing transaction speed. The same solution can also approve the transactions automatically if they meet the predetermined conditions.

As a result, audit preparations become easier as policies and decisions are made and managed centrally while being external to the applications.

2 Delegation for special use cases

Almost every financial institution currently leverages role-based access control (RBAC) which assigns permissions based on the role within the organization. However, the RBAC lacks the ability to delegate permissions for special and unique cases. An example of such a case might include a financial audit, accessing personal financial records or accessing loan management records.

To overcome this challenge, you can deploy attribute-based access control (ABAC), which establishes fine-grained permissions based on a variety of variables and attributes, which can include role, location, etc.

This approach extends beyond the roles used in existing business processes by adding a delegation attribute which defines who the authority is delegated to, what they can access and for how long.

3 Relationship management

Financial institutions will want to protect their customers' financial data from being shared with employees who have a relationship with the customer.

To achieve this, institutions can check to see if the account that is going to be accessed is under the scope of what their employees' permissions are. For example, an account manager would only be able to open the accounts which they are responsible for.

4 Anomalous behavior detection and response

In any financial institution, it is important to identify any user behaviors associated with fraud and immediately terminate access.

In 2022, Flagstar Bank announced that hackers gained unauthorized access to their networks and more than 1.5 million customer records. Incidents like this one can be caused by employee errors, employees, negligence, and data theft by malicious insiders.

This can be solved by implementing decision-making policies that describe the anomalous behavior based on a variety of scenarios. It can also trigger a denial of access to the user once those conditions are met to protect the system.

5 Data sharing and regulation compliance

Banks and financial institutions face the ongoing challenge of complying with data protection and privacy regulations when it comes to personal identifiable information (PII). These regulations include the General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX), and the Payment Card Industry Data Security Standard (PCI DSS). According to SailPoint, less than half of respondents, with the exception of NIST, say they are confident with their organization's ability to be compliant.

To protect the data, an authorization solution can enact policies that trigger other tools in your environment to take actions such as data masking and encrypting data. Therefore, the policies release customer data only under strict need-to-share basis and ensure compliance with data protection regulations.

6 Big data analysis

Another challenge is to perform business analysis. This can be difficult to achieve without compromising compliance because there are different regulations for data use based on different countries.

At the heart of an ABAC policy decision is a question about the permissions and entitlements a particular subject has when accessing data. Because of this, you can ensure consistent controls are applied regardless of what applications are being used to request the data. As a result the sensitive data is de-identified while remaining discoverable, searchable and sortable.

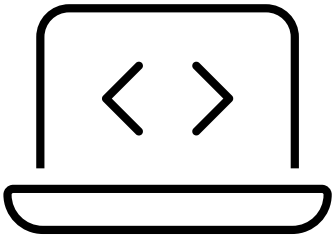
7 Separation of Duty (SoD)

Lastly, investment banks may face the challenge of wanting to eliminate the risk of 'rogue traders' engaging in speculative trading without authorization.

Using an ABAC solution can help control access, approvals and reduce other behaviors that indicate speculation. This helps the bank allow a trader to approve a transaction only if they did not initiate the transaction. It can also be used to prevent SoD violations in cases where the policy stated a trader could initiate a transaction for a client if they had not previously initiated a similar transaction in the last ten hours for a competing client.

Why Axiomatics

Since 2006, Axiomatics has provided authorization solutions to many of the world's leading banks and financial institutions. We provide a policy and attributed-based approach to access control that can be used at multiple layers including databases, Big Data, applications, APIs, and microservices.



See why so many financial institutions across the globe have used our authorization solutions.

Request a demo with one of our solution experts to see our award-winning offering in action.

Cost amounts in this article are measured in US dollars (USD).

Policy-based access control solutions for enterptise

Axiomatics has been solving the challenge of authorization for organizations since 2006. Their solution and proven approach simplifies the orchestration of fine-grained authorization to organization's applications, information, and processes via a central, dynamic, Zero Trust policy engine. This centralized approach removes the burden of coding and managing authorization functionality for each application separately while ensuring a consistent set of compliance and security policies are properly engaged across the organization.

For more information or to request a demo, please visit **axiomatics.com**.

About Axiomatics

Axiomatics is the originator and leading provider of runtime, fine-grained, dynamic authorization delivered with Attribute Based Access Control (ABAC) for applications, data, APIs, and microservices.

The world's largest enterprises and government agencies use the Axiomatics Dynamic Authorization Suite to enable digital transformation, share and safeguard sensitive information, meet compliance requirements and minimize data fraud. Our innovative solutions enable enterprises to share sensitive, valuable and regulated digital assets – but only to authorized users and in the right context.

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240

AXIOMATICS