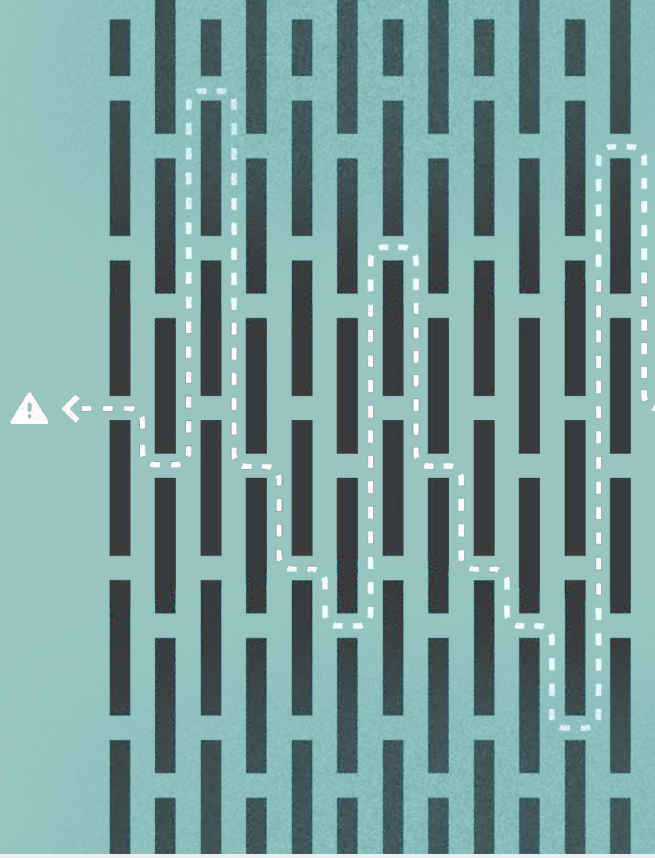
The Bank Secrecy Act (BSA), enacted in 1970, was the United States' first major legislation to combat money laundering and financial crimes.

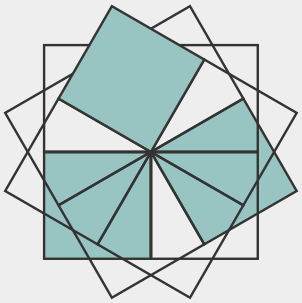


It aimed to detect and prevent illegal activities by requiring banks to maintain certain records and report specific transactions. Over time, its mandates expanded to address terrorist financing, tax evasion, and other illicit activities. The Act has faced criticism for being burdensome on financial institutions due to extensive reporting requirements. Nonetheless, it's recognized as a vital tool in the government's effort to combat financial crime. The BSA's effectiveness is debated, but it has undeniably changed the landscape of financial oversight and regulatory compliance.

The BSA mandates rigorous recordkeeping and reporting standards for financial institutions. This ensures transparency and provides a trail for investigating illicit activities. BSA's emphasis on robust internal controls implies a need for:

1. Advanced security measures
2. Routine audits
3. Regular employee training to protect sensitive information

Bank Secrecy Act (BSA) Components Relevant to Email & Cloud Environments



The BSA's provisions instruct that organizations must safeguard sensitive data, especially when stored in emails or documents, to prevent breaches and maintain compliance. Such data, if compromised, can expose institutions to regulatory penalties and reputational harm.

Mandate	Citation	Description	Implication	Material's Solution
Recordkeeping	31 USC § 5313	Financial institutions must keep records of certain transactions, including those above a specified value.	Requires robust data storage and retention mechanisms.	Identify relevant messages, secure those messages by redacting the content, ensure proper access via authentication, and maintain audit logs.
Currency Transaction Report (CTR)	31 USC § 5313	Institutions must report cash transactions exceeding $10,000 in one business day.	Sensitive data like names, addresses, and transaction details are stored.	Secure and encrypt emails with sensitive data, employ robust access controls, and monitor transactions.
Suspicious Activity Report (SAR)	31 USC § 5318(g)	Institutions must report suspicious transactions that might signify money laundering, tax evasion, or other illegal activities.	Involves identifying potentially illicit activities.	Use a combination of pre-built and custom-built detections to identify suspicious activity and streamline triage activities.. Instantly search and report for real-time analysis and reporting.
Customer Due Diligence (CDD)	31 CFR § 1010.230	Institutions must identify and verify the identity of customers, understanding the nature and purpose of customer relationships.	Data about customers, their activities, and their associations may be stored in emails.	Identify PII stored in emails and after an appropriate amount of time redact the content of those emails in order to secure the content in the case of a breach.