coinbase INSTITUTE

EXPLAINER

How zero-knowledge proofs can bring the Bank Secrecy Act into the digital age

TLDR: The Bank Secrecy Act's AML system was built for a paper era. This means that banks collect the same sensitive data over and over—increasing costs and the risk of breaches, and triggering a flood of low-value reports. Zero-knowledge proofs (ZKPs) can fix this by letting institutions prove that customers and transactions meet AML rules without exposing underlying sensitive information, enabling reusable identity credentials, increased privacy, and better data. ZKPs have the potential to modernize the financial system and benefit consumers in everything from cross-border payments to correspondent banking and beyond. To enable this technology, regulators should update BSA rules to recognize the use of ZKPs, and work with industry to set clear standards and support pilot projects.

The Bank Secrecy Act (BSA) has anchored America's anti-money laundering framework for more than fifty years. Enacted in 1970, it requires financial institutions to verify customer identities and monitor transactions for suspicious activity. These obligations were designed for an era when money moved by paper check and compliance meant filing forms in triplicate. Today, the pace and scale of financial activity have changed dramatically, yet the law's implementation remains tethered to outdated practices. As a result, the BSA leads to massive amounts of personal data collection, redundant checks, and reports that often go unread. While its purpose remains critical, the system is inefficient, privacy-invasive, and poorly suited for the digital age.

Modern cryptography offers a way forward. Zero-knowledge proofs (ZKPs) are a breakthrough technology that allows one party to prove that a statement is true without revealing the underlying information. Instead of repeatedly handing over sensitive personal data to dozens of institutions, individuals can use a single proof that verifies they meet regulatory requirements without exposing more than what is necessary. This shift would preserve the integrity of compliance while dramatically improving privacy, efficiency, and security.

Understanding KYC within the BSA framework

Know Your Customer (KYC) requirements form the foundational pillar of BSA compliance. Under the Customer Identification Program (CIP) rules, financial institutions must verify the identity of anyone opening an account by collecting specific information: name, date of birth, address, and identification number. But KYC extends far beyond this initial verification.

The BSA's KYC obligations include:

Customer due diligence (CDD): Institutions must understand the nature and purpose of customer relationships and conduct ongoing monitoring to identify and report suspicious transactions. This requires maintaining current customer information and monitoring account activity patterns.

Enhanced due diligence (EDD): For higher-risk customers, such as politically exposed persons (PEPs) or those from high-risk jurisdictions, institutions must conduct deeper investigations including understanding the sources of funds and wealth.

Beneficial ownership: For legal entity customers, institutions must identify and verify the beneficial owners who ultimately control the entity, creating complex webs of documentation and verification.

The Current Challenge

A single customer opening accounts at five different banks must provide identical personal information five times, creating five separate databases containing the same sensitive data—multiplying breach risks by five.

This multi-layered approach creates enormous data collection requirements. Each institution independently verifies the same information, stores it in separate databases, and monitors the same customers across multiple relationships. The result is a system where personal financial data is duplicated dozens of times across the financial system, creating security vulnerabilities and inefficiencies that ZKPs could elegantly address.

How zero-knowledge proofs work

ZKPs function by separating validation from disclosure. In contrast to today's system, they allow a trusted provider to confirm the relevant information and generate cryptographic proof of compliance. The proof, not the underlying data, is what customers share with a new institution.

Zero Knowledge Proofs

Think of ZKPs like a mathematical "black box" that can answer "yes" or "no" to compliance questions without revealing the underlying supporting data. The box might confirm "this person is over 18 and not on sanctions lists" without revealing their actual age or identity.

Because the proof is mathematically verifiable, the receiving institution can be certain the conditions are satisfied without seeing the raw data itself. The individual's sensitive details remain private, while the compliance obligation is fully met. If law enforcement later needs to investigate a particular case, it can subpoena the original ZKP provider to access the underlying information. This model ensures accountability without turning every customer into a potential data point for endless storage and review.

The same principle can be applied to transaction monitoring. Today, financial institutions monitor all transactions and generate millions of reports to the Treasury Department each year. Most contain little useful information, and the volume is so overwhelming that many reports are never analyzed. With ZKPs, institutions could generate proofs that certain transactions meet objective reporting thresholds, transmitting only the relevant cryptographic attestations to regulators. Instead of collecting oceans of personal data, agencies would receive cleaner, more targeted signals. Combined with advanced analytics, this approach would improve the detection of illicit activity while reducing the noise and redundancy of current processes.

Expanded use cases for zero-knowledge proofs in BSA compliance

1. **Enhanced transaction monitoring**

ZKPs would allow institutions to provide regulators with proof that suspicious activity thresholds are met without disclosing unrelated personal data about law-abiding customers. Regulators could then apply machine learning and pattern recognition techniques to standardized proofs, improving their ability to detect sophisticated networks of illicit activity.

2. **Cross-border payments compliance**

Currently, cross-border payments often require institutions to share extensive customer data to satisfy different jurisdictions' AML/KYC requirements. ZKPs could allow a bank to prove "this customer has been properly verified according to jurisdiction A's standards" without revealing the underlying personal information, customer transaction history, or specific verification methods used.

3. **Beneficial ownership verification**

For complex corporate structures, ZKPs could prove that beneficial ownership has been properly identified and verified without exposing the complete ownership chain to every institution. This is particularly valuable for legitimate privacy-sensitive entities like family offices or corporations with competitive concerns about ownership disclosure.

4. **Regulatory examination efficiency**

During BSA examinations, regulators could use ZKPs to verify that institutions have properly conducted required due diligence without needing to review every individual customer file. Examiners could receive cryptographic proofs that KYC procedures were followed, dramatically reducing examination time while maintaining oversight effectiveness.

5. **Sanctions screening optimization**

Instead of sharing full customer lists with sanctions screening services, institutions could use ZKPs to prove screening was conducted against current lists without exposing customer identities to third-party screening vendors. This would address growing concerns about data sharing with external compliance vendors.

6. **Correspondent banking relationships**

ZKPs could revitalize correspondent banking relationships by allowing smaller institutions to prove their BSA compliance standards meet correspondent bank requirements without sharing detailed customer information. This could help restore banking access to underserved communities affected by de-risking practices.

Efficiency Gains

Some industry estimates suggest ZKP-based compliance could reduce KYC costs by more than a quarter while improving data security and regulatory effectiveness.

Implementation considerations

The transition to ZKP-based BSA compliance would require coordination between regulators, financial institutions, and technology providers. Key considerations include:

- Standardization: It is important that regulatory agencies establish standards for acceptable ZKP implementations and trusted credential providers.
- Infrastructure: Widespread adoption would also require interoperable systems within the financial industry for generating, transmitting,

and verifying ZKPs across different platforms and institutions.

- Scalability: Ensuring that ZKP systems are optimized for speed and scalability, through advances in proof generation and verification, is key for practical use.
- Legal Framework: Existing BSA regulations should be updated to explicitly recognize ZKPs as acceptable methods of compliance verification.
- Audit Trails: Systems must maintain sufficient audit capabilities to support law enforcement investigations while preserving privacy benefits.

Conclusion

The Bank Secrecy Act remains a cornerstone of U.S. financial integrity, but its execution is stuck in the past. Requiring every institution to collect, store, and transmit sensitive personal information is both risky and ineffective. Zero-knowledge proofs provide a modern alternative: one that modernizes our financial systems and brings real benefits to consumers.

Policymakers should encourage the adoption of ZKPs within BSA compliance frameworks, allowing institutions to meet their obligations without perpetuating the inefficiencies of a paper-based era.

By embracing this technology, the financial system can become more secure, more efficient, and more privacy-respecting while detecting illicit activity more effectively than ever before.

The question is not whether zero-knowledge proofs will transform financial compliance, but how quickly regulators and institutions will embrace this opportunity to modernize a system that has served its purpose but is ready for its next evolution.

The Path Forward

Policymakers should encourage pilot programs using ZKPs within BSA compliance frameworks, starting with low-risk use cases like identity portability between banks within the same holding company.

Note: This material is for informational purposes only, and is not (i) an offer, or solicitation of an offer, to invest in, or to buy or sell, any interests or shares, or to participate in any investment or trading strategy, (ii) intended to provide accounting, legal, or tax advice, or investment recommendations or (iii) an official statement of Coinbase. Coinbase may have financial interests in, or relationships with, some of the entities discussed or referenced in the materials. Coinbase does not endorse or approve links or third-party websites that may be provided in the materials.