algemetric

Secure Multi-Party Computation in BFSI: Unlocking Collaborative Analytics for Risk & Compliance

Executive Summary

C-level executives and compliance officers in Banking, Financial Services, and Insurance (BFSI) face a dual challenge: harnessing data for better decision-making while upholding strict privacy and regulatory standards. Secure Multi-Party Computation (commonly called SMPC or MPC) is emerging as a game-changing privacy-enhancing technology that allows institutions to jointly analyze sensitive data without ever exposing or centralizing that data (linkedin, dualitytech). This white paper outlines how Algemetric's MPC solutions can drive strategic value in four critical BFSI use cases:

- **Privacy-Preserving Credit Risk Evaluation:** Multiple lenders can collaboratively assess creditworthiness or portfolio risk by pooling insights without sharing raw customer data. This approach yields a more accurate risk profile while maintaining client confidentiality (linkedin.com, khazna.ku.ac.ae).
- **AML Collaboration & Joint Monitoring (Bank–Telecom):** Banks and telecom operators can share transaction patterns and anti-money laundering (AML) intelligence to detect illicit finance that spans financial and mobile networks. MPC enables *"scenarios without borders"* in AML (dualitytech) – identifying suspicious activity across institutions – all while complying with privacy laws.
- **Secure Reconciliation & Audit Across Subsidiaries:** Global financial groups can perform cross-border reconciliations, compliance checks, and audits between subsidiaries using MPC. This ensures consistency and regulatory reporting accuracy (e.g. sanction screening or capital limit checks) without violating data localization or privacy regulations (bis.org, linkedin).
- **Privacy-Preserving Fraud Detection & Benchmarking:** Institutions can jointly detect fraud schemes and benchmark fraud rates or other performance metrics against peers without revealing competitive data. By securely pooling indicators of fraud, firms gain a collective defense advantage and insight into their relative performance (linkedin).
- **Payment Tokenization & Settlement**: Banks, merchants, and payment networks can jointly tokenize and analyze payment data for settlement, reconciliation, or loyalty programs, without exposing underlying transaction details.

These use cases reflect the real barriers BFSI firms face today: data silos, regulatory conflict, lack of secure collaboration mechanisms, and pressure to modernize securely. Traditional tools,

such as centralized data lakes, anonymized extracts, or trusted intermediaries, fall short. MPC offers a fundamentally different, privacy-respecting foundation. In short, MPC allows financial consortia to “unlock the power of data to tackle major challenges, from international money laundering to pandemics, in a way that respects citizens’ rights” (NIST).

Algemetric’s innovations address prior performance barriers, enabling these privacy-preserving analyses to be done efficiently on real-world financial data. This means BFSI leaders cannot choose between analytics and privacy – they can have both. The following sections break down each use case, real-world examples, and the value propositions in an executive-friendly manner.

Introduction: Privacy-Enhancing Collaboration in BFSI

Today, BFSI institutions are expected to act on data while complying with strict data protection laws (e.g., GDPR, data residency statutes). But regulatory and structural barriers make inter-organizational collaboration difficult. As a result, fraud goes undetected, credit is under- or over-extended, and risk decisions are made on incomplete information. Institutions often say, “We are only seeing 25% of our customers’ banking activity... the majority happens outside our walls” (Oracle).

MPC solves this by letting institutions collaborate *without sharing* sensitive data. It allows computations over encrypted or secret-shared data inputs, where no party can learn the others’ inputs—only the result. Privacy-enhancing technologies (PETs) like MPC are now being promoted by regulators (e.g., UK-US PETs Challenge, FATF) as a tool to both enhance data collaboration and uphold data rights (NIST).

Algemetric’s implementation overcomes the main blockers seen in early-stage MPC—namely, performance, decimal accuracy, and integration complexity. Our Mercury MPC engine and PIE encoding technology support financial-grade precision and seamless deployment.

Use Case 1: Privacy-Preserving Credit Risk Evaluation

Challenge: Risk data is fragmented across banks, credit bureaus, and fintechs. Sharing data outright violates privacy rules or antitrust laws. Without collaboration, credit risk assessments remain incomplete or skewed, particularly for underbanked populations or borrowers with non-traditional financial histories.

Traditional Limitation: Anonymization reduces model accuracy. Centralized scoring exposes data custodians to compliance risk. Moreover, aggregating credit data at a central location introduces both a technical bottleneck and a concentration of regulatory liability.

MPC Solution: MPC allows multiple lenders or data holders to jointly compute credit scores, risk models, or aggregate insights without exposing inputs. For example, two banks assessing a

mutual client can combine their insights without revealing data to each other. This enables broader visibility into a customer's repayment behavior, outstanding liabilities, or collateral status, which is crucial when no single institution has the full picture.

Cited Precedent: Abbe, Khandani, and Lo (2011) demonstrated this concept in their seminal work, proposing privacy-preserving methods for financial risk analysis using MPC (arXiv). More recently, Credora began offering real-time credit risk scoring over encrypted data (Credora), allowing crypto lenders and trading platforms to operate with transparency while preserving privacy.

Strategic Impact: This enables more accurate and inclusive lending, supports shared risk modeling, and levels the playing field between large and small institutions. It also empowers credit consortia and underwriters to engage in joint portfolio stress testing, collaborative exposure analysis, and ecosystem-wide credit simulations.

Use Case 2: Collaborative AML Monitoring Between Banks and Telecoms

Challenge: Money laundering often spans multiple banks and telecoms. Each institution sees only a fragment of the transaction trail. Yet legal, operational, and technical barriers prevent joint analysis, especially between entities governed by distinct regulatory regimes.

Traditional Limitation: Manual data-sharing frameworks (e.g., 314(b) in the U.S.) are slow, heavily restricted, and require trust between institutions. Telecom operators, despite handling mobile payments and SIM-based financial activities, are often excluded from traditional financial crime detection frameworks.

MPC Solution: MPC enables banks and telecoms to jointly analyze customer activity and transaction metadata (e.g., location, device ID, frequency of SIM swaps) to uncover suspicious patterns. Each party retains its data locally but can contribute securely to a shared analysis, such as detecting fast-moving funds tied to phone numbers associated with synthetic identity fraud.

Real-World Proof: The MPC4AML project in the Netherlands demonstrated that multiple financial institutions could collaboratively detect laundering patterns through secure graph-based analysis while preserving privacy (ERCIM). The Cyber Defence Alliance in the UK and tech sprints hosted by the FCA also highlight the growing interest in PETs for cross-sector intelligence sharing.

Strategic Impact: This expands AML effectiveness into adjacent data ecosystems (telecom, crypto, fintech), enables faster risk flagging and interdiction, and opens the door to privacy-safe data fusion across industries. It also signals to regulators a proactive stance on collaborative financial crime prevention.

Use Case 3: Secure Reconciliation and Audit

Challenge: Global financial firms face increasing pressure to reconcile transactions, account balances, and compliance reports across geographies. Yet data localization laws, internal data silos, and risk of breach make traditional reconciliation processes slow and incomplete.

Traditional Limitation: Manual reconciliation across subsidiaries is labor-intensive and error-prone. Relying on third-party aggregators can introduce compliance concerns and reduce data sovereignty. Many institutions struggle to reconcile group-wide exposures, reserve requirements, and sanctions lists without violating cross-border data restrictions.

MPC Solution: MPC allows separate entities (e.g., a parent and its subsidiaries, or a regulated bank and its affiliates) to verify that records match or that exposure thresholds are met without revealing underlying data. This enables compliance-by-design workflows where participants prove compliance without exposing sensitive records.

Cited Project: Project Mandala by the BIS used MPC to validate cross-border capital flows and enforce capital restrictions while keeping transaction-level data private (BIS).

Strategic Impact: Reduces audit lag, eliminates manual file exchange, and helps satisfy increasingly complex jurisdictional mandates. Also enables central compliance or risk teams to proactively monitor exposure and reporting without direct access to localized PII or transactional data.

Use Case 4: Privacy-Preserving Fraud Detection and Industry Benchmarking

Challenge: Fraudsters increasingly operate across multiple platforms, banks, fintechs, and telecoms, exploiting gaps between data silos. Meanwhile, financial institutions are limited in their ability to share incident data or benchmark against peers due to privacy, regulatory, and reputational constraints.

Traditional Limitation: Firms hesitate to participate in shared blacklists or fraud databases due to legal risk. Benchmarking metrics like fraud rates, false positive ratios, or alert conversion are often considered too sensitive to publish or exchange.

MPC Solution: MPC allows institutions to detect fraud patterns across networks, such as identifying shared device fingerprints, IP addresses, or account behaviors, without exposing internal logs. It also supports secure benchmarking: firms can compare fraud metrics (e.g., average chargeback rate) and receive percentile-based feedback without revealing proprietary statistics.

Real-World Adoption: The Cyber Defence Alliance piloted privacy-enhancing methods for joint fraud investigations, and regulators in the UK and US have explicitly encouraged secure data collaboration for financial crime prevention. The FCA's PETs TechSprint in 2019 highlighted fraud typology sharing as a prime use case for MPC and homomorphic encryption.

Strategic Impact: Enables fraud intel sharing without exposing internal controls or case files. Promotes ecosystem-wide learning and accountability while safeguarding competitive advantage and customer privacy.

Use Case 5: Payment Tokenization & Settlement

Challenge: The secure exchange, reconciliation, and enrichment of payment data across banks, merchants, and payment networks is critical, but it is plagued by fragmented infrastructure, inconsistent standards, and stringent privacy requirements. Transaction-level transparency is needed to fuel services like loyalty programs, chargeback investigations, and real-time settlement, yet exposing raw transaction data creates risk.

Traditional Limitation: Existing tokenization approaches focus on security at rest and in transit, but don't enable shared analytics or insight generation without compromising confidentiality. Settlement and reconciliation processes remain batch-based, error-prone, and siloed.

MPC Solution: MPC enables secure collaborative analysis of tokenized payment data across institutional boundaries. Banks, merchants, and payment processors can jointly compute on encrypted or secret-shared data, for example, to match transactions across systems, validate loyalty criteria, or generate aggregate payment insights, without exposing underlying transaction records.

Strategic Impact: Improves the efficiency and accuracy of cross-party settlement and reconciliation workflows. Supports privacy-preserving personalization of customer rewards. Creates a compliant foundation for payment data collaboration that can scale across card networks, merchants, and banking institutions.

Addressing Adoption Barriers

Adoption of MPC in BFSI has historically been limited by several concerns that go beyond pure cryptographic maturity:

- **Technical complexity:** Many earlier MPC solutions were designed by and for cryptographers. They required deep knowledge of secure computation protocols, circuit design, or homomorphic logic, none of which align with the skill sets of typical IT or risk professionals.
- **Performance:** Prior platforms struggled with latency, floating-point operations, and memory usage. This made them unsuitable for financial applications requiring decimal precision, near real-time response, or large-scale parallelism.

- **Integration pain:** Legacy banking infrastructure often relies on rigid architectures, batch processing pipelines, and incompatible formats. Without easy integration hooks, MPC platforms were seen as exotic rather than practical.
- **Compliance uncertainty:** Institutions were hesitant to deploy tools they couldn't easily explain to regulators or auditors. The absence of defined legal frameworks around MPC exacerbated this caution.

How Algemetric Solves These:

- **Performance:** Our Mercury protocols have been optimized to perform operations on decimals, enabling BFSI operations.
- **Ease of use:** We are building an intuitive tooling that abstracts away cryptographic complexity, enabling analysts and compliance teams to use MPC workflows without specialized training.
- **Compliance-first architecture:** Our platforms designed to include detailed event logging, audit trails, and jurisdictional enforcement mechanisms to align with regulations like GDPR, HIPAA, and PSD2.
- **Enterprise integration:** APIs and deployment patterns for hybrid IT landscapes.

Call to Action: Unlock the Next Phase of Secure Collaboration

Secure Multi-Party Computation (MPC) has moved beyond theory and into practical application. The question is no longer "can this be done?", but rather, "who will lead the way?"

At Algemetric, we believe that MPC represents a strategic opportunity for financial institutions to become pioneers in a new era of privacy-preserving collaboration. It is not just a technology; it is an enabler of compliance-aligned innovation, resilient infrastructure, and responsible data sharing.

We invite forward-thinking executives, data governance leaders, and compliance strategists to join us in shaping what comes next. Whether your institution is exploring fraud detection, AML collaboration, secure benchmarking, or audit automation, MPC offers the foundation to act decisively and without compromising privacy or control.

Algemetric is actively seeking BFSI partners to:

- Pilot regionally tailored solutions built with performance, jurisdictional awareness, and regulatory rigor.
- Shape the product roadmap for the next generation of privacy-first financial infrastructure.
- Demonstrate leadership in adopting PETs and setting new standards for collaboration in the industry.

Together, we can build workflows that are efficient, auditable, and defensible, delivering insight while preserving trust.

Contact us to join our partnership programs, explore joint innovation opportunities, or learn more about how MPC can power your institution’s next move.