

Information Technology in Financial Services: A Dual-Edge Analysis Transformative Opportunities and Critical Vulnerabilities in Modern Banking

Pankaj Kumar

Former Technical Lead, Tata Consultancy

Abstract - Information Technology has fundamentally reshaped the financial services industry, creating unprecedented opportunities for efficiency and accessibility while introducing complex vulnerabilities and systemic risks. This paper examines both dimensions through empirical evidence and technical analysis across ten critical domains of financial services operations. Drawing from twenty years of hands-on experience and industry data, we provide a balanced assessment of IT's dual-edge role in modern banking. Our analysis reveals that IT creates 70-90% cost reductions and financial inclusion for 1.7 billion people, yet simultaneously introduces \$288 billion in annual fraud losses and systemic fragilities. The research demonstrates that successful institutions must view technology as a complex risk-benefit calculation requiring constant recalibration, substantial security investment, and commitment to serving diverse populations. We conclude that the path forward requires embracing IT's transformative power while developing robust frameworks to manage its capacity for systemic disruption.

Keywords - Information Technology, Financial Services, Cyber security, Digital Transformation, Fin Tech, Risk Management, Payment Systems, Regulatory Compliance

I. INTRODUCTION

The financial services industry stands at a remarkable crossroads. Technology offers powerful tools for improving efficiency and expanding access, yet the industry faces profound technological risks from cyber attacks to system failures that can paralyze economies. This contradiction is intrinsic to how modern IT systems operate.

This research stems from twenty years of implementing anti-money laundering systems, fraud detection platforms, and regulatory compliance technologies for major financial institutions. I've witnessed both the transformative benefits and the failures that emerge. This paper documents both sides of that story.

A. Historical Context and Evolution

The financial services industry has undergone four major technological revolutions:

Mechanization Era (1950s-1970s): Introduction of mainframe computers for basic record-keeping. Bank of America's ERMA system (1955) and ACH networks (1970s) enabled electronic funds transfers, though batch processing meant days-long settlement times.

Digitization Era (1980s-1990s): ATMs proliferated, electronic trading replaced physical trading floors, and core banking systems evolved to handle multiple products. Credit card networks introduced real-time authorization, fundamentally changing payment dynamics.

Internet Era (2000s-2010s): Online and mobile banking transformed customer relationships. Algorithmic trading dominated markets (60-70% of equity volume by 2010). Yet this era also brought new risks - the 2008 crisis was partly enabled by algorithmic trading complexity, and data breaches exposed millions of records.

Intelligence Era (2015-Present): AI makes autonomous credit and fraud decisions. Blockchain promises to restructure settlement. Open banking forces data sharing through APIs. This era raises questions about algorithmic bias, AI explainability, big tech concentration, and system stability.

Each revolution amplified both opportunities and risks exponentially. New technology creates efficiency gains, institutions rush to adopt it, dependencies deepen, and only later do risks and unintended consequences become apparent.

B. Research Objectives

This paper has three primary objectives: First, provide comprehensive analysis of where IT delivers the most significant benefits, quantified with empirical data. Second, identify and analyze critical vulnerabilities and risks IT introduces. Third, offer insights for navigating this dual-edge reality through appropriate governance and operational practices.

We examine ten domains where IT's impact is most pronounced: Payment Systems, Credit Risk Assessment, Fraud Detection, Regulatory Compliance, Customer Experience, Trading Infrastructure, Data Security, Operational Efficiency, Financial Inclusion, and Systemic Risk Management.

C. Methodology

This research draws from multiple sources: twenty years of direct experience implementing compliance systems at major institutions, published academic and industry research, empirical data from regulatory reports, specific case studies of successes and failures, and technical analysis of underlying architectures.

The analysis is deliberately balanced. Technology creates genuine value and genuine risks. Both deserve careful examination.

II. DOMAIN ANALYSIS: OPPORTUNITIES AND CHALLENGES

A. Payment Systems and Transaction Processing

1) Where IT Provides Biggest Help

Real-time payment systems represent one of the most significant infrastructure advances. Traditional batch processing meant days-long settlement. Modern systems process continuously (24/7/365), enabling instant settlement, cross-border transactions in seconds versus days, microtransaction viability, and multi-currency processing with real-time conversion.

Measurable impact: Processing speed declined from 1-3 days to under 10 seconds. International remittance costs dropped from 10% to under 1% in advanced corridors. Visa processes 65,000 transactions/second versus 7 for Bitcoin. The World Bank reports 1.7 billion previously unbanked adults gained access through digital payments.

Case Study - UPI India: Launched 2016, UPI processes 10+ billion monthly transactions (\$200+ billion value). Cost per transaction: \$0.0002 versus \$0.50-1.00 for cards. Success factors: open APIs, mandated interoperability, zero merchant fees. Impact: Hundreds of millions joined digital economy, small merchants accept payments through QR codes, transaction data enables credit scoring for populations without banking history.

2) Where IT Creates Biggest Challenges

Single Points of Failure: Centralization creates cascading vulnerabilities. October 2021 Visa outage affected Europe for hours due to one data center failure. TSB Bank's 2018 migration failure locked 1.9 million customers out for weeks, costing £330 million.

Settlement Risk: Real-time payments eliminate fraud detection buffers. Once paid, funds are irrevocable. UK APP fraud reached £485 million in 2022 - victims authorize payments to criminal accounts, systems can't distinguish from legitimate transfers.

Infrastructure Dependencies: Payment systems depend on complex infrastructure. The 2016 SWIFT breach at Bangladesh Bank resulted in \$81 million theft, revealing that attacks on weakest links compromise entire networks.

B. Credit Risk Assessment and Lending

1) Benefits

Automated credit scoring revolutionized lending. Statistical models trained on historical data evaluate creditworthiness in seconds versus days. Models consistently outperform human loan officers in predicting defaults. Alternative data (utility payments, mobile usage, digital footprints) enables credit scoring for populations without traditional histories. Kenya's M-Pesa uses mobile transaction data for credit scoring, providing access to millions previously excluded.

Machine learning creates dynamic risk assessments updating continuously. Portfolio stress testing simulates performance under adverse scenarios - capabilities essential for post-2008 regulatory requirements.

2) Challenges

Algorithmic Bias: Models trained on biased historical data perpetuate discrimination. The 2019 Apple Card controversy showed algorithms creating gender-based outcomes without explicitly considering gender - correlation with other factors produced discriminatory results.

Opacity: Machine learning "black boxes" make accurate predictions but can't explain why. This creates fairness concerns - how can borrowers improve if they don't know what algorithms assess? How can regulators evaluate discrimination they can't understand?

Systemic Risk: Common model dependencies create system-wide exposure. The 2008 crisis showed how similar flawed assumptions about mortgage risk spread problems across the entire financial system.

C. Fraud Detection and Prevention

1) Benefits

Real-time transaction monitoring using machine learning achieves 30-50% better accuracy than rule-based systems. Behavioral analytics identify deviations from individual customer patterns. Network analysis detects fraud rings operating across supposedly unrelated accounts. Device fingerprinting and biometric authentication significantly reduced account takeover fraud.

2) Challenges

Sophisticated Attacks: Synthetic identity fraud - creating fictitious identities that appear legitimate over months/years before "busting out" - doesn't follow detectable patterns. No real victim reports fraud until bust-out occurs.

False Positives: Balancing fraud detection with customer convenience is challenging. Excessive fraud prevention creates terrible customer experiences. Different institutions make different risk-friction trade-offs.

Privacy Concerns: Effective fraud detection requires analyzing enormous behavioral data, creating privacy concerns. GDPR and CCPA limit data collection, potentially reducing fraud detection effectiveness.

D. Regulatory Compliance and Reporting

1) Benefits

Automated compliance monitoring makes feasible what manual review couldn't achieve at scale. From my experience implementing these systems, modern AML platforms use machine learning for subtle pattern recognition, network analysis for money laundering detection, and entity resolution for identifying individuals operating multiple accounts under different names.

Regulatory reporting automation extracts data from multiple systems, applies required calculations, formats per specifications, and submits electronically. Without automation, banks would need armies of accountants at prohibitive cost.

KYC automation verifies identity against authoritative sources in seconds versus hours of manual research.

2) Challenges

Regulatory Complexity: Global operations require handling conflicting jurisdictional requirements. Systems must understand jurisdiction-specific rules and maintain audit trails. Large banks spend hundreds of millions annually on compliance technology, requiring constant updates as regulations change.

False Positives: Compliance teams review tens of thousands of monthly alerts, most proving innocuous. Investigation costs are substantial - not just salaries but opportunity costs from investigating false positives versus genuine risks.

Barrier to Entry: Compliance technology costs create barriers favoring large institutions. Smaller institutions and startups struggle with fixed costs prohibitive relative to revenue, reducing competition and innovation.

E. Customer Experience and Digital Banking

1) Benefits

24/7 accessibility eliminated branch visit requirements. Mobile check deposit exemplifies transformation - photograph deposits versus driving to branches. Instant account visibility helps customers manage finances effectively. Personalized product recommendations use spending data to suggest relevant products. Automated financial management tools (spending tracking, budgeting, savings goals) democratize advice previously available only to wealthy clients.

2) Challenges

Digital Divide: Elderly, disabled, digitally illiterate, and those without reliable internet struggle with digital banking. As branches close, these populations find access diminished. The customers needing most help face greatest exclusion from digital-first models.

Cybersecurity Risks: Digital banking exposes customers to phishing, account takeover, malware, and social engineering. Banks depend on customers following security practices many lack knowledge to implement.

Technology Failures: When digital banking fails, customers have no alternative access. Major banks experienced high-profile outages preventing account access for hours or days.

Impersonal Service: Digital banking struggles with situations requiring human judgment, empathy, or complex problem-solving. Algorithms can't replicate nuanced assistance or comprehensive financial planning.

F. Trading and Market Infrastructure

1) Benefits

Electronic trading revolutionized markets. Transaction costs declined 75% over two decades. Market liquidity increased. Algorithmic execution optimization helps institutional investors achieve better prices. Market data democratization created more level playing fields - individual investors access tools previously requiring expensive professional terminals.

2) Challenges

Flash Crashes: May 6, 2010 - Dow plunged 1,000 points in minutes then recovered. Automated sell orders overwhelmed liquidity, high-frequency algorithms withdrew, cascading crisis sent stocks to \$0 or \$100,000 - clearly erroneous but system-generated. Circuit breakers now prevent similar crashes, but fundamental fragility from automated trading remains.

Market Manipulation: "Spoofing" (placing orders intended for cancellation to create false demand/supply) exploits electronic trading speed and anonymity. Detection requires sophisticated surveillance algorithms; proving intent is challenging.

Technology Arms Race: Speed advantages create questions about market fairness. High-frequency firms locate servers in exchange data centers (microsecond advantages), run fiber through mountains (latency reduction). Does technology dependency favor large firms over smaller participants?

G. Data Security and Privacy

Modern encryption protects data in transit and at rest. Multi-layered security (network, application, access control, monitoring, incident response) means breaches of one control encounter additional defenses. However, financial institutions are prime breach targets. Equifax (2017) exposed 147 million people; Capital One (2019) affected 100 million customers. Breaches cost not just direct response but regulatory fines, lawsuits, and reputational damage.

Insider threats, ransomware, and supply chain risks (2013 Target breach via HVAC vendor; 2020 SolarWinds compromise) create additional vulnerabilities. Securing decades of legacy data against sophisticated attackers is extraordinarily difficult.

H. Operational Efficiency and Cost Reduction

Straight-through processing automates end-to-end operations without human intervention. Process automation delivers 70-90% cost reductions. Cloud computing shifts from capital to operating expenditure, enabling scale-up/down flexibility. Robotic Process Automation handles repetitive tasks 24/7 at fraction of human cost.

However, technical debt from decades-old legacy systems creates substantial challenges. Integration is difficult and expensive. Maintenance costs increase as workforce knowing legacy technologies retires. Yet replacement is risky - TSB's £330 million migration failure demonstrates risks, but continuing with decades-old systems creates security and integration problems.

Implementation costs are substantial - tens to hundreds of millions for large projects, with 50-70% failing to meet objectives, deliver late, or get abandoned. Cybersecurity costs hundreds of millions annually. Vendor dependency creates lock-in risks, particularly with cloud providers.

I. Financial Inclusion and Access

Mobile money transformed developing countries. Kenya's M-Pesa (launched 2007) serves 50+ million customers. Research shows M-Pesa access improved household welfare and lifted hundreds of thousands from poverty. Women particularly benefited - mobile money gave financial control and enabled savings groups. China's Alipay/WeChat Pay and India's UPI achieved similar scale.

Neobanks with no branches offer services at lower cost, enabling previously unprofitable customer segments. No minimum balances, no monthly fees, no overdraft fees - genuinely transformative for low-income customers previously paying hundreds annually in banking fees.

Challenges include the digital divide (elderly, disabled, digitally illiterate struggle), predatory lending through mobile apps with illegal interest rates and aggressive collection, data privacy concerns (every transaction recorded and potentially monetized), and fraud victimization of newly banked populations lacking experience recognizing scams.

J. Systemic Risk and Crisis Management

Technology enables stress testing required post-2008 - banks must demonstrate survival under severe scenarios. Real-time systemic risk monitoring tracks liquidity, lending rates, trading volumes. Network analysis maps interconnections that could trigger cascading problems.

However, technology failures themselves become systemic risks. Common dependencies (shared cloud providers, payment networks) could affect many institutions simultaneously. Cybersecurity threats could destabilize financial systems if critical infrastructure were compromised. Algorithmic trading might exacerbate rather than stabilize stressed markets. Concentration in few technology providers creates systemic vulnerabilities.

III. SYNTHESIS AND COMMON THEMES

A. Efficiency Versus Resilience Trade-Offs

IT optimizes for efficiency, often at resilience expense. Modern systems eliminate redundancy that was inefficient but provided alternatives during failures. Traditional systems had manual processes providing fallbacks. Modern systems often have no alternatives - when digital banking fails, customers are stranded; when payment networks fail, transactions can't process; when trading systems crash, markets halt entirely. This trade-off is fundamental. Resilience requires redundancy, spare capacity, alternative procedures - all costing money and reducing efficiency. Financial pressure pushes toward efficient systems with limited resilience.

B. Automation of Risk versus Creation of New Risks: IT automates risk management (fraud detection, credit scoring, compliance monitoring) often performing better than human judgment for well-defined problems. However, automation creates new risks - algorithmic systems fail unexpectedly, exhibit unrecognized biases, create fragility through interconnections, and make errors at scale impossible with manual processes.

IT doesn't simply reduce risk - it transforms risk. Traditional risks are mitigated while new technology-specific risks emerge. Net effect depends on implementation quality, ongoing security investment, and governance frameworks.

C. Inclusion Versus Exclusion Dynamics

Technology dramatically expanded access for some (mobile banking in developing countries, digital lending for subprime borrowers, robo-advisors for middle market) while creating new exclusions (elderly, digitally illiterate, those without reliable internet find traditional access diminished as branches close). IT is simultaneously the most significant financial inclusion driver in history and a creator of new exclusions. Both effects are real and significant.

D. Centralization and Systemic Interdependence

IT enables centralization - fewer, larger platforms serving more customers; common standards enabling interoperability; concentration in major technology companies and cloud providers. This creates efficiency through economies of scale and network effects but also systemic interdependencies where central system failures cascade across entire ecosystems. Traditional fragmentation limited contagion. The move toward centralized, interconnected infrastructure created efficiency gains but increased systemic risk not fully understood or managed.

E. The Paradox of Technological Progress

Analysis across all domains reveals a fundamental paradox: IT is simultaneously the greatest enabler and the most significant vulnerability in modern financial services. This isn't temporary - it's intrinsic to how IT transforms systems. Technology creates value through speed, scale, interconnection, and automation. But these same characteristics create vulnerability. Faster systems leave less time for intervention. Larger scale means failures affect more people. Greater interconnection means problems cascade further. More automation means errors propagate at machine speed.

The appropriate question isn't "should we adopt technology?" (competitive pressure makes adoption inevitable) but "how do we capture benefits while managing risks and maintaining resilience?"

IV. KEY FINDINGS AND QUANTITATIVE RESULTS

A. Value Creation

IT creates remarkable value: 70-90% cost reductions in transaction processing, financial inclusion for 1.7 billion previously unbanked individuals, 30-50% improvement in fraud detection accuracy, transaction times reduced from days to seconds, approximately \$50 billion in annual savings across global banking.

B. Vulnerabilities Introduced

IT introduces serious vulnerabilities: single points of failure disabling entire payment networks, \$288 billion in annual losses from digital fraud and cybersecurity incidents, \$700+ million failures in system migrations, digital exclusion affecting 15-20% of populations, regulatory compliance costs forcing industry consolidation and reducing competition.

C. Key Insights

First, IT transforms rather than reduces risk. Technology mitigates traditional risks while introducing new technology-specific risks. Net effect depends heavily on implementation quality, ongoing security investment, and governance.

Second, efficiency gains require continuous investment to sustain. Upfront gains can be dramatic, but maintaining them requires ongoing spending on security, maintenance, modernization, and resilience. Institutions capturing efficiency while underinvesting accumulate vulnerabilities manifesting as costly failures.

Third, benefits and risks are unevenly distributed. Technology creates enormous value for tech-savvy populations while potentially excluding others. Large, well-capitalized institutions manage challenges more effectively than small community banks.

Fourth, systemic interdependencies are not fully understood. Dependence on few technology providers, platforms, and infrastructure creates concentration risks with potential systemic consequences. Comprehensive management frameworks remain under development.

Fifth, competitive pressure makes technology adoption inevitable. Customers expect digital capabilities, regulators require sophisticated compliance technologies, operating costs without modern technology become prohibitive. The question isn't whether to adopt but how to manage associated risks.

V. IMPLICATIONS FOR STAKEHOLDERS

A. For Financial Institutions

Technology is Not Optional: Competitive pressure, customer expectations, and regulatory requirements make adoption inevitable. Resistance means losing market share and failing to meet evolving expectations. Security and Resilience Require Ongoing Investment: Efficiency gains are real, but sustainable capture requires continuous cybersecurity investment, system resilience, disaster recovery, and operational redundancy. Underinvestment creates existential risks that will eventually materialize.

Digital Inclusion Requires Deliberate Effort: Market forces alone exclude vulnerable populations. Institutions valuing diverse customer bases must deliberately maintain capabilities serving those unable to use digital channels.

Technical Debt Must Be Managed: Accumulated technical debt eventually becomes competitive and operational liability. Institutions need long-term strategies addressing legacy systems rather than indefinitely extending lifespans.

Risk Transformation Requires New Governance: Traditional frameworks (credit risk, market risk, operational risk) must expand to address technology-specific risks - cyber risk, model risk, algorithm risk, vendor risk, systemic technology interdependencies.

Vendor Dependencies Need Strategic Management: Increasing reliance on third-party providers requires maintaining negotiating leverage, avoiding lock-in where possible, ensuring vendor security and resilience, and having contingency plans for vendor failures.

B. For Regulators and Policymakers

Technology-Specific Regulation Is Necessary: Traditional banking regulation (capital adequacy, liquidity, credit quality) is insufficient. Regulators need frameworks specifically addressing cybersecurity, technology resilience, algorithm governance, data protection, and vendor oversight.

Systemic Technology Risk Requires Attention: Regulators have sophisticated frameworks for systemic risk from financial interconnections but have been slower addressing systemic risk from technology dependencies. Concentration of financial services on few cloud providers, payment networks, and platforms creates systemic vulnerabilities requiring attention.

Innovation and Competition Must Be Balanced with Safety: Technology enables new business models and competitors driving innovation and improving customer service. However, regulatory barriers (compliance costs disproportionately burdening small institutions) can reduce competition. Regulators must balance fostering innovation with maintaining safety and soundness.

Consumer Protection Frameworks Need Updating: Traditional consumer protection doesn't always fit digital financial services. Algorithmic bias, digital exclusion, data privacy, and online fraud require updated frameworks.

International Coordination Is Essential: Financial services operate globally, technology enables borderless delivery. Fragmented national regulations create arbitrage opportunities and make comprehensive oversight difficult. Greater international coordination would improve effectiveness.

VI. LOOKING FORWARD

The trajectory is clear: financial services will continue becoming more technology-driven. Several trends will further transform the industry: Artificial Intelligence will increasingly make autonomous decisions about credit, fraud, customer service, and risk management, raising questions about bias, explain ability, and accountability. Block chain and distributed ledger technology may restructure clearing and settlement, potentially reducing costs and settlement times while introducing new technical and governance challenges.

Open Banking will continue expanding, forcing institutions to share customer data with third parties through APIs, creating opportunities for innovation and new security/privacy concerns. Cloud Computing will become the dominant infrastructure model, concentrating enormous portions of the financial system on handful of cloud platforms operated by big tech companies.

Quantum Computing will eventually threaten current encryption standards, requiring entire financial system migration to quantum-resistant cryptography - a massive, costly, risky undertaking. Each development will bring benefits and create new vulnerabilities, continuing the dual-edge pattern characterizing IT's impact throughout history.

VII. CONCLUSION

A. The Paradox of IT in Financial Services

Information Technology stands as both the greatest enabler and the most significant vulnerability in modern financial services. This dual nature isn't contradictory but inevitable - the same characteristics creating efficiency, accessibility, and innovation also generate systemic fragility, concentration risk, and cascading failure points. Our analysis reveals consistent patterns. IT creates remarkable value: 70-90% cost reductions, financial inclusion for 1.7 billion people, 30-50% improvement in fraud detection, transaction times reduced from days to seconds, approximately \$50 billion in annual savings globally. Simultaneously, IT introduces serious vulnerabilities: single points of failure, \$288 billion in annual losses from digital fraud and cybersecurity, major system migration failures, digital exclusion affecting 15-20% of populations, compliance costs forcing consolidation and reducing competition.

B. Final Assessment

Information Technology in financial services represents not a choice between opportunity and risk, but an ongoing management challenge where both dimensions intensify simultaneously.

Successful institutions must: View technology implementation not as pure efficiency play, but as complex risk-benefit calculation requiring constant recalibration. Invest substantially in security, resilience, and disaster recovery, recognizing these as essential enabling investments rather than overhead costs. Maintain commitment to serving all customer segments regardless of digital capability, recognizing financial inclusion requires deliberate effort beyond market forces. Develop governance frameworks specifically for technology risks, including cyber risk, model risk, algorithm governance, and vendor risk management. Manage technical debt strategically rather than deferring costly but necessary system modernization indefinitely. Balance efficiency benefits of vendor-provided solutions with strategic risks of dependency and lock-in. The path forward requires embracing IT's transformative power while respecting its capacity for systemic disruption. This balance - capturing technology's benefits while managing its risks - will define financial services stability and success for decades to come.

The dual-edge nature of IT in financial services isn't a problem to be solved, but a fundamental characteristic to be managed. Success requires sophistication, investment, attention, and humility about what we don't yet know about the systems we've built. The stakes are high - the stability of the global financial system and the financial welfare of billions of people depend on how well we navigate this dual-edge reality.

ACKNOWLEDGEMENT

This research draws from two decades of experience implementing financial compliance and fraud detection systems at major financial institutions, as well as extensive review of academic literature, industry reports, and regulatory guidance.

REFERENCES

- [1] Financial Stability Board, "FinTech and Financial Innovation: Implications for Regulation and Supervision," December 2023.
- [2] World Bank Group, "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19," 2022.
- [3] Bank for International Settlements, "Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors," February 2018.
- [4] European Banking Authority, "Report on the Impact of FinTech on Incumbent Credit Institutions' Business Models," July 2018.
- [5] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 2018.
- [6] Committee on Payments and Market Infrastructures, "Fast Payments - Enhancing the Speed and Availability of Retail Payments," November 2016.

- [7] McKinsey & Company, "Global Banking Annual Review 2024," 2024.
- [8] UK Finance, "Fraud: The Facts 2024: The Definitive Overview of Payment Industry Fraud," 2024.
- [9] International Monetary Fund, "Fintech: The Experience So Far," June 2019.
- [10] Federal Reserve Board, "Financial Stability Report," November 2023.
- [11] Lewis, M., "Flash Boys: A Wall Street Revolt," W.W. Norton & Company, 2014.
- [12] Philippon, T., "The FinTech Opportunity," NBER Working Paper 22476, August 2016.
- [13] Berg, T., et al., "On the Rise of FinTechs: Credit Scoring Using Digital Footprints," *The Review of Financial Studies*, Vol. 33, July 2020.
- [14] Gomber, P., et al., "On the Fintech Revolution," *Journal of Management Information Systems*, Vol. 35, 2018.
- [15] Vives, X., "Digital Disruption in Banking," *Annual Review of Financial Economics*, Vol. 11, 2019.
- [16] Suri, T., and Jack, W., "The Long-Run Poverty and Gender Impacts of Mobile Money," *Science*, Vol. 354, December 2016.
- [17] O'Neil, C., "Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy," Crown Publishing, 2016.
- [18] Kirilenko, A., et al., "The Flash Crash: High-Frequency Trading in an Electronic Market," *The Journal of Finance*, Vol. 72, June 2017.
- [19] Arner, D.W., et al., "The Evolution of Fintech: A New Post-Crisis Paradigm?" *Georgetown Journal of International Law*, Vol. 47, 2016.
- [20] Zetsche, D.A., et al., "From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance," *European Banking Institute Working Paper 2018-No. 6*, February 2018.