

Technology Expands into Financial Services Accelerating Digital Finance and Creating Dynamic Data Footprints

Since the Passing of the USA PATRIOT Act, Technology has Reshaped Financial Services from Centralized Bank Branch Storefronts to Online Digital Platforms and Mobile Apps

Installment Four of a Six-Part Series

September 2026

From Paper Trails to Predictive Algorithms

The Recurring Gap Between Innovation and Regulation

Financial-crime regulation has consistently followed technological change rather than anticipated it. Three overlapping cycles have reshaped anti-money laundering (AML) and countering the financing of terrorism (CFT), Bank Secrecy Act (BSA), and sanctions law since the 1990s: (1) computers and the internet (1990s–2001), (2) digital payments and blockchain (2000s–2020s), and (3) artificial intelligence (AI) (2020s–present). The technology changes, but the pattern remains: innovation creates new vulnerabilities, financial crime adapts, and regulation responds.

2001: The Turning Point

The September 11 attacks exposed a critical convergence: financial networks, modern communication systems, and global movement of funds could be exploited to facilitate transnational terrorism. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (USA PATRIOT Act) transformed the regulatory response by bringing financial crime, technology, and national security into a more integrated framework. It expanded the government's ability to trace financial transactions, access financial and electronic records, and disrupt illicit financial flows associated with terrorism and money laundering.

Technology Significantly Expands the Data Footprint

The pattern did not end with the USA PATRIOT Act. As financial technology evolved and new forms of illicit activity emerged, regulators repeatedly adapted the legal and compliance framework to address new risks. The emergence of digital platforms enabled access to extensive customer data to provide support in meeting regulatory obligations.

“

*Prior to the USA PATRIOT Act, law enforcement had been operating at a technological disadvantage in the war against terrorism. Agents often were forced to use outdated legal authorities to fight terrorists who were using modern technology. In short, we were **waging a 21st century war with mid-20th century weapons**.*

*The USA PATRIOT Act's modernization of federal law falls into three broad categories. First, the Act gives federal officers **new tools to fight terrorists who use modern technologies** to plot their attacks. Second, it **enhances existing investigative tools, such as wiretaps and pen register and trap and trace (“pen/trap”) devices**, to bring them up-to-date with changing technology. And third, the USA PATRIOT Act helps officials to obtain the cooperation of third parties, such as communications providers, in the war against terrorism.*

- Report from the Field: The USA PATRIOT Act at Work, Department of Justice (July 2004)

”



Shifting Gears in Regulatory Landscape



PERSONAL COMPUTERS / WORLD WIDE WEB (1990s–2001)

*The PATRIOT Act updated the law to match current technology, so that we no longer have to fight a 21st-century battle with antiquated weapons. **Terrorists exploit modern technology such as the Internet and cell phones to conduct and conceal their activities.** The PATRIOT Act leveled the playing field, allowing investigators to adapt to modern techniques.*

- Robert S. Mueller III, Director, Federal Bureau of Investigation, Before the United States Senate Committee on the Judiciary Washington DC (May 24, 2004)



FINANCIAL TECHNOLOGY (2000s–2020s)

*The financial system is undergoing **fast-moving changes associated with digitalization and decentralization.** Some of these innovations hold considerable promise to **reduce transaction costs and frictions, increase competition, and improve financial inclusion,** but there are also potential risks. With technology driving profound change, it is important we **prepare for the financial system of the future and not limit our thinking to the financial system of today.***

- Governor Lael Brainard, Member of the Federal Reserve Board of Governors (February 18, 2022)



ARTIFICIAL INTELLIGENCE (2020s–PRESENT)

*Innovations in AI, including machine learning and large language models, such as generative AI, have significant **potential to strengthen AML/CFT compliance by helping financial institutions analyze massive amounts of data and more effectively identify illicit finance patterns, risks, trends, and typologies.** Financial institutions, federal financial regulators and policy makers should leverage these workstreams to inform possible uses of AI-driven AML/CFT compliance tools in a safe, secure, and trustworthy manner.*

- Department of the Treasury 2024 National Strategy for Combating Terrorist and Other Illicit Financing)



2001: Technology, Finance & National Security Converge

The USA PATRIOT Act connected the financial system to the emerging realities of a technology-driven threat environment. Its provisions expanded access to information, strengthened identity controls, and modernized investigative capabilities—creating a broader framework for following the money, the people, and the communications behind financial crime and terrorism.

Section 314: Information Sharing

Created mechanisms for financial institutions and government to exchange information on suspected money laundering or terrorist financing.

Section 361: Formalized FinCEN as a Treasury Bureau

Strengthened FinCEN's statutory authority and role as the US financial intelligence unit responsible for combating money laundering and terrorist financing.

Section 214 & 216: Electronic Investigative Tools

Expanded pen-register and trap-and-trace authorities to cover electronic communications, including email, modernizing investigative tools to reflect the growing use of digital communications in financial and criminal investigations.

Section 326: Customer Identification Program

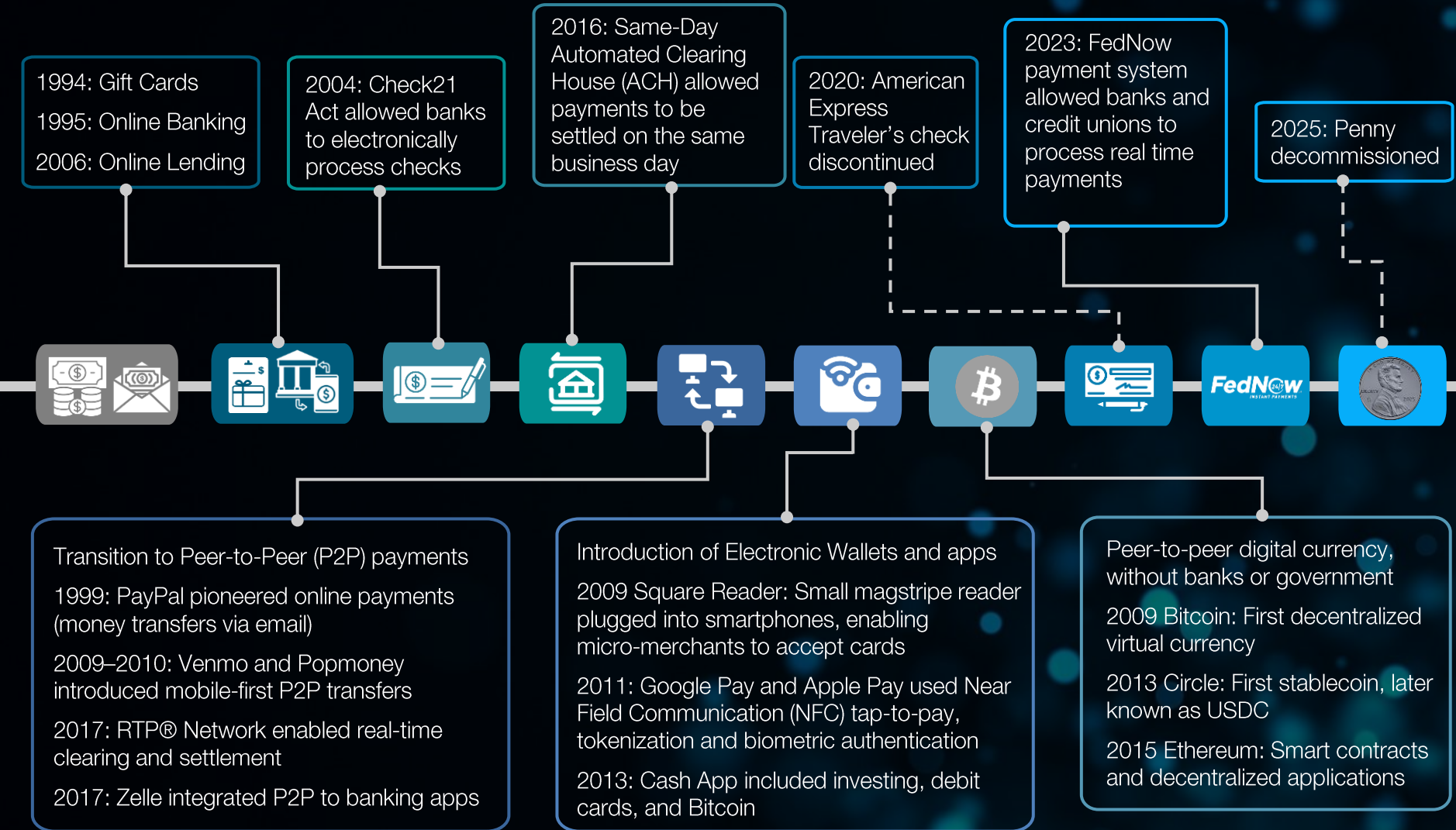
Established customer identification program (CIP) requirements for banks, strengthening the link between identity, account, and transaction.

Tech Impact:

Advances in technology allowed for the use of secure email, document sharing and portal access systems, and messaging, among others, to efficiently and effectively share information.



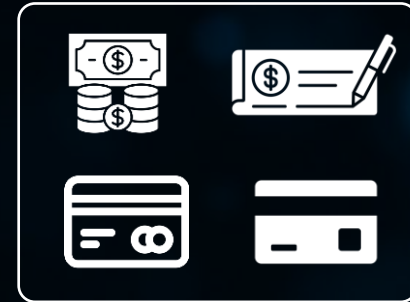
25 Years: Technology Advances from Ledgers to Logins



Wallet Evolution: From Bifold to Passcode, What's in your Wallet?

Pocketable Tradition

Physical wallets used to be the primary means for carrying personal and financial essentials, such as cash, checks, debit and credit cards, and identification credentials. As most transactions were in-person or required photo or signature verification, carrying cash, instruments, and identification was essential.



The Move to Contactless Age

The emergence of digital wallets and smartphones provided a faster, secure, and convenient way to manage personal and financial essentials. Reliance on traditional wallets and payment methods decreased as preferences shifted to contactless transactions through multifunctional apps used for document storage, card credentials, linked bank accounts, and P2P services.

2026



The Deliberate Use of Cash

Cash becomes an infrequent and an inefficient transaction method as retail checkouts are card-based, provide digital transaction history, and a seamless purchase. Now, using cash is a deliberate transaction to avoid today's data footprint that is inherent in digital transactions.



Technology Facilitates Rapid Advancements in Financial Services

Technology reshaped banking by moving from branch-based systems to application programming interface (API)-driven digital platforms. Customers prioritize speed and convenience, preferring mobile apps, online transfers, and contactless payments. At the same time, social media accelerates the shift by broadcasting instant feedback on products and services, directly influencing customer decisions when opening accounts or conducting transactions.

Payments: Speed of Movement

Shorter or real-time transaction, clearing, or settlement of funds



- Instant Transfers
- Real-time Settlement
- Tap-to-Pay and Mobile Apps
- QR Checkout
- Cross-Border Transactions

Physical vs. Digital Footprint

Paper documents to digital information



- Digital ID and Biometric Liveness
- Browsing History, Cache, Cookies
- Online Verification
- Automated Screenings
- API Automation

Dynamic Banking Relationship

Transition to uncoupled banking



- Service-Specific
- Lesser Fee % or Higher Rates
- Online Offers
- Data-Driven Services
- Social Media Influence



25 Year Data Snapshot from Static to Dynamic Footprint

Under the USA PATRIOT Act's original CIP standard, compliance relied on a fixed set of documents, a static, point-in-time verification model. Today, identity has become a continuous data stream rather than a fixed file, encompassing biometric authentication, geolocation, digital payments, behavioral monitoring, and social activity. Compliance programs built on the original documentary static standard now face a customer profile that is dynamic, constantly generated, and with an extensive data footprint.

2001: Static Footprint

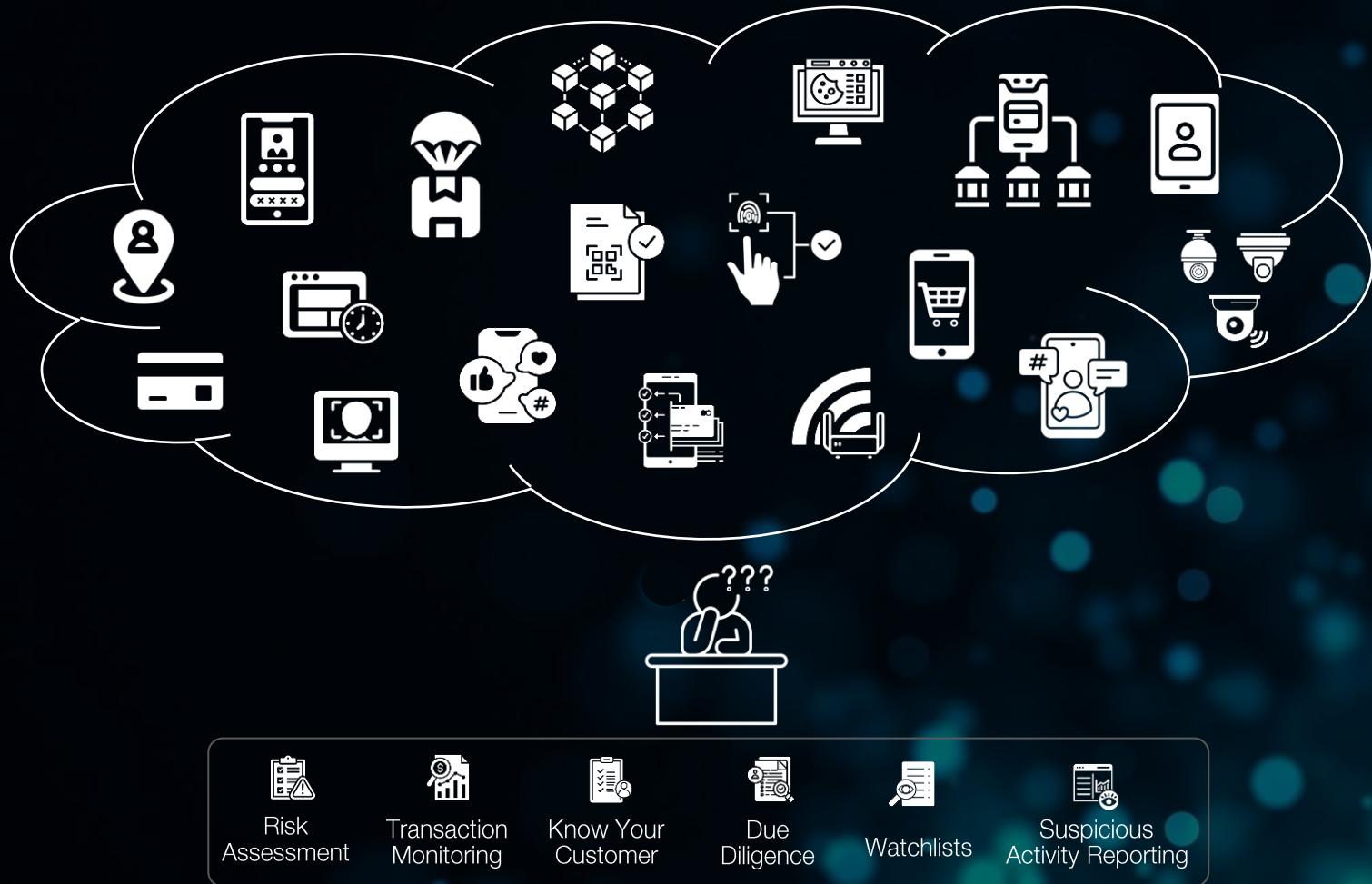


2026: Dynamic Footprint



Dynamic Footprint: Too Much Information to be Effective?

The various amount of customer data collected through different methods and channels can pose as an opportunity or challenge to compliance teams. When data is not effectively shared and operationalized, it remains siloed, limiting the compliance team's insights for the detection of risks and hinder efficient compliance functions. The challenge is whether compliance teams have access to all the customer dynamic data and utilize it effectively in their due diligence, monitoring, and reporting requirements.



25 Years Later, Technology Continues to Shape Financial Services

Technology is reshaping the regulatory and operating environment for financial institutions. The reliance on manual processes and limited data to perform compliance obligations has declined. Technology has opened new opportunities and challenges for financial institutions in strengthening their oversight and risk management practices.

The underpinnings of the USA PATRIOT Act will be challenged in the next evolution of financial services. Expansion in the digital assets marketplace continues, while AI is an emerging critical driver with real use cases rolling out and broad-scope adoption on the horizon. Network heavy reliance and persistent cyber threats have necessitated the appointment of a dedicated Chief Information Security Officer (CISO), like the establishment of the Compliance Officer requirement under the BSA.

Finally, technology firms are embedded in the regulated financial services marketplace and now are acquiring community banks to fast-track access to bank charters that provide a broader opportunity for customer acquisition and growth.

Digital Assets



Governance



Transparency



Risk-based
Monitoring



Traceability
and Regulatory
Alignment

Cybersecurity



Unified Controls



Threat Detection



Integrated
Frameworks



Data
Consolidation
and Integrity

Artificial Intelligence



Automated
Monitoring



Human-in-
the-loop



Machine
Learning



Early Detection
and Error
Reduction

Tech Bank Acquisitions



Product
Expansion



Leaner
Approach



API and AI
Driven



Buy-a-Charter





StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

LAUNCH | SCALE | OPTIMIZE

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com