Rocket® software

Modern Banking Demands Real-Time Security

Closing Access Gaps in Core Banking Systems

Introduction

The financial services landscape is evolving rapidly. Customer expectations for digital convenience, shaped by fintech innovators, are at an all-time high. In response, banks are accelerating their modernization efforts, but this transformation introduces significant risks. As you adopt new technologies, your attack surface expands, exposing decades-old infrastructure – particularly core banking systems accessed via green screens – to increasingly sophisticated threats.

At the same time, regulatory bodies are intensifying their scrutiny, introducing new mandates that challenge traditional security models. Legacy access controls, once considered sufficient, are now creating critical security gaps. This guide explores how evolving financial fraud schemes and new regulatory obligations are exposing these vulnerabilities and outlines the compliance priorities that will shape the banking industry in 2026-2027. We'll provide a clear path forward, helping you close these access gaps and secure your most critical operations.

The shifting threat landscape: New fraud schemes targeting banks

The core systems that power banking – mainframes and other backend host systems – are the ultimate targets for cybercriminals. These platforms process billions of transactions daily and store vast amounts of sensitive customer data. While historically secure, the methods used to access them are now a primary vector for attack. Evolving fraud schemes are specifically designed to exploit the weaknesses of traditional terminal emulator access.

Real-world scenarios and emerging threats:

Authorized push payment (APP) fraud:

This scheme tricks customers or employees into sending money to fraudulent accounts. Criminals often use social engineering to gain credentials, then exploit weak access controls on host systems to manipulate payment details or create synthetic identities. A bank teller with compromised credentials could inadvertently approve a fraudulent transfer, with the weak authentication process on the green screen offering no secondary validation.

Deepfake identity fraud:

AI-powered deepfakes are becoming alarmingly convincing. Fraudsters can use this technology to impersonate legitimate customers during video verification or even mimic the voice of a senior executive to authorize large transactions. If the final approval happens on a system that relies solely on a simple password, there's no defense against this sophisticated attack vector.

Insider threats & credential stuffing:

Disgruntled employees or external actors with stolen credentials pose a significant risk. Without multi-factor authentication (MFA) or session monitoring on host system access, it's nearly impossible to distinguish a legitimate user from a malicious one. A single compromised password can give an attacker direct access to core banking functions, enabling them to siphon funds, steal data, or disrupt operations.

Evolving regulatory obligations: What to expect in 2026-2027

Regulators are keenly aware of these emerging threats and are moving quickly to mandate stronger security controls. The focus is shifting from perimeter defense to a Zero Trust architecture, where every access request must be continuously verified. Banks that don't adapt will face significant fines, reputational damage, and operational disruption.

Key compliance priorities for 2026-2027:

01

Strengthened identity and access management (IAM):

Regulations like the Digital Operational Resilience Act (DORA) in the EU and directives from the New York State Department of Financial Services (NYDFS) are mandating robust IAM. For banks, this means extending modern authentication practices like MFA and single sign-on (SSO) to all systems, including mainframes. Relying on simple, eight-character passwords for green screen access will no longer be compliant. Regulators expect banks to prove that only authorized users can access critical data, and legacy emulators often can't provide this level of assurance.

02

Mandatory third-party risk management:

The banking ecosystem is increasingly interconnected, with third-party vendors and fintech partners often requiring access to core systems. Future regulations will hold banks directly responsible for breaches originating from their partners. You must have the ability to enforce consistent security policies and monitor all sessions, regardless of who is accessing the system or from where. A centralized access management solution becomes essential for demonstrating compliance.

03

Comprehensive audit and reporting trails:

In the event of a breach, regulators will demand a complete record of who accessed what, when, and why. Traditional terminal emulators often lack the detailed logging capabilities needed to provide this evidence. For 2026-2027, banks will need to implement solutions that offer centralized, immutable audit trails for every user session on their host systems. This not only aids in forensic investigations but also serves as proof of compliance during audits.

What happens if you fall short?

Non-compliance or a detected gap can result in failed audits, large fines, forced remediation, and reputational damage – making proactive modernization a regulatory imperative.

Closing the gap: Modernizing access to core banking systems

The convergence of sophisticated fraud and stringent regulations creates an urgent need to modernize host access. The solution isn't to "rip and replace" the time-tested systems that run your bank, but to secure the pathways to them.

Rocket® Secure Host Access™ helps you bridge this critical gap. By integrating your green screen applications with modern IAM platforms, you can enforce the same robust security policies across your entire enterprise.

How to build a more resilient bank:

01

Extend MFA & SSO to the mainframe

Eliminate the risk of compromised passwords by integrating host access with your existing IAM solution. This ensures every user is properly authenticated before they can access core banking applications.

02

Achieve centralized control & visibility

Manage all user sessions from a single pane of glass. A modern approach allows you to enforce granular access policies, monitor for suspicious activity in real time, and terminate sessions instantly if a threat is detected.

03

Streamline compliance & audits

Automatically generate detailed session logs that provide irrefutable evidence for auditors. This simplifies compliance reporting and strengthens your security posture by leaving no activity unrecorded.

04

Empower adoption & productivity

A user-friendly approach ensures high adoption rates and a smoother transition for staff – minimizing disruption and accelerating your path to compliance.

Conclusion: Secure your future by securing your core

The banking industry is at a critical juncture. The same legacy systems that provide unparalleled reliability are now at risk due to outdated access methods. As financial fraud becomes more advanced and regulations more demanding, waiting to address these security gaps is no longer an option.

By rethinking how your organization connects to core banking systems, you can overcome evolving security threats and regulatory demands with confidence. Rocket® Secure Host Access™ is designed to help you close critical access gaps, streamline compliance, and strengthen your resilience against fraud — all while supporting seamless integration and high user adoption. Protect the heart of your banking operations and ensure you're ready for the challenges of 2026 and beyond.

Learn more about Rocket® Secure Host Access™ & how it can future-proof your institution.

About Rocket Software

Rocket Software is a global technology leader in modernization and a partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,200 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-17720_WP_SHABankingGuide_V2