

ActivIdentity Banking and Financial Services Solutions

Build customer trust and address compliance challenges



Benefits

- Build customer trust and confidence across electronic service channels
- Extend reach by securing mobile service channels
- Minimize insider threats to information assets and systems
- Enforce internal security policies related to local and remote access
- Increase revenue by introducing new, more secure online services
- Improve security and manage costs by matching authentication strength to transaction risk
- Strengthen compliance with government regulations and industry mandates
- Reduce fraud-related losses by using strong authentication for employees, suppliers, and customers

The financial services industry has experienced significant changes in the last decade. These changes have led to new service delivery channels, consolidation of large and medium-size institutions, and more stringent regulations. As banks and other financial institutions enhance online and mobile channels in response to user demand, they must successfully manage internal and external risks. Strengthening security and compliance is a key challenge facing the industry. ActivIdentity solutions enable financial institutions to improve security and compliance by centralizing disparate authentication systems, securing internal access, and extending strong authentication to customers.

Industry Trends and Challenges

Financial services institutions have undergone a revolution in recent years. Early in the decade, a critical mass of Internet and wireless usage sparked a profusion of new service offerings, including online banking, electronic payments, and bill-pay alternatives to check writing. At the same time, significant deregulation allowed banks and other financial services institutions to combine to offer a range of products (e.g., savings, investments, and insurance) to consumers and businesses. The recent financial crisis accelerated the pace of acquisitions. The resulting industry consolidation, a renewed emphasis on regulation, and growth of organized cyber crime and insider threats have left over-taxed risk managers, security officers, information technology (IT) staff, and line-of-business personnel scrambling to address a long list of security challenges, while operating with fewer resources.

Online Retail Banking Testimonial

"CFS researched the market for an appropriate provider. ActivIdentity's industry-leading expertise, highly efficient support for EMV CAP authentication, and the ability to use the same authentication infrastructure for multiple business units were key reasons behind our decision to appoint them."

- **Tony Britten**, Director of Financial Crime Management, *Co-operative Financial Services*

Funds Transfer for Institutional Investors And Insurers Testimonial

"ActivIdentity offered a perfect solution and a good investment in the future because it delivered the highest level of security available with a reusable infrastructure."

- **Johan van der Wal**, Manager Client Information, *KAS BANK*

At a time when it is critical to rebuild customer trust and confidence in the financial services industry, many organizations are at increased risk of external data breaches and internal data thefts. Adding to the burden, rapid change has bred the proliferation of disparate security systems (both for employees and customers) throughout organizations. Besides the management and maintenance issues of such an environment, demonstrating compliance (see table 1) is more complex when multiple authentication systems, each with its own activity logs, are deployed. The prospect of consolidating authentication for a variety of internal and external user communities poses an additional challenge to financial institutions in the face of increasing risk management and compliance costs.

Table 1. Financial Services Compliance Overview

Regulation or Industry Mandate	Purpose
Payment Card Industry (PCI) Data Security Standard	Protect card holder data from internal and external breaches (includes eliminating default and shared passwords; supporting password timeouts and failed-attempt lockouts; and enforcing password change on first-time use)
Federal Financial Institutions Examination Council (FFIEC) Guidance	Provide guidance on authentication for Internet banking (requires stronger forms of authentication beyond static passwords)
Fair and Accurate Credit Transactions (FACT) Act	Combat identity theft and maintain the privacy of financial transactions
Health Insurance Portability and Accountability Act (HIPAA)	Maintain the privacy of health care-related transactions
Gramm-Leach-Bliley Act (GLBA)	Protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to customers
Sarbanes-Oxley Act (SOX)	Disclose any significant deficiency in the internal control structure and / or any fraud perpetrated by any individual with a significant role related to internal controls

Mobile and Online Trends and Challenges

Banks, brokerage firms, payment providers, and insurers are responding to consumer and corporate customer expectations for convenient services that allow them to conduct financial transactions from any location.

- **Consumers:** While consumers demand mobile access to account information and everyday tasks, they also want richer, more productive experiences on the Web. New entrants in the market are offering full-featured Web 2.0 user interfaces that consolidate data from several accounts into a single view. Banks are racing to launch their own web “dashboards” even as they realize that a single point of access for several accounts increases risks.
- **Corporate customers:** Corporate banking customers are also demanding web-based, value-added services. These services include funds transfer and cash management tasks that require strong authentication and non-repudiation. Matching authentication strength to transaction risk – while minimizing user inconvenience – requires organizations to provide a range of versatile authentication options.

ActivIdentity Solutions

ActivIdentity Strong Authentication and Credential Management solutions help financial services institutions improve security and demonstrate compliance while reducing the costs and complexity of risk management. Using ActivIdentity solutions, organizations can strengthen the security of electronic interactions across multiple channels, as well as centralize the auditing and reporting of authentication and authorization across diverse user communities. ActivIdentity Strong Authentication and Credential Management solutions address the range of transaction risk levels, flexibly accommodate multiple authentication mechanisms and devices, and support full user and credential life cycle management.

ActivIdentity Banking and Financial Services Customers

- BNP Paribas
- Co-operative Financial Services (CFS)
- Federal Reserve Bank of New York
- Fiserv
- Hana Financial Group
- KAS BANK N.V.
- SNS Bank

Americas +1 510.574.0100
US Federal +1 571.522.1000
Europe +33 (0) 1.42.04.84.00
Asia Pacific +61 (0) 2.6208.4888
Email info@actividentity.com
Web www.actividentity.com

About ActivIdentity

ActivIdentity Corporation (NASDAQ: ACTI) is a global leader in strong authentication and credential management, providing solutions to confidently establish a person's identity when interacting digitally. For more than two decades the company's experience has been leveraged by security-minded organizations in large-scale deployments such as the U.S. Department of Defense, Nissan, and Saudi Aramco. The company's customers have issued more than 100 million credentials, securing the holder's digital identity.