

## ACI Drives Adoption of Multifactor Authentication Solutions

(SAN FRANCISCO, Calif. - RSA Conference – 6 February, 2007) – ACI Worldwide (NASDAQ: TSAI), a leading international provider of software for electronic payment systems, today announced 18 financial institutions are deploying ACI Enterprise Banker™ software with enhanced multifactor authentication features to combat increasingly sophisticated online banking threats. ACI is the first enterprise software vendor to launch live customers on the RSA Go IDSM authentication service. Additionally, ACI announced that 14 banks are deploying the RSA Adaptive Authentication for Web risk-based authentication technology at application logon, and several of the company's bank customers will be implementing the Enterprise Banker solution with integrated multi-part credentials from TriCipher.

“With the rapid increase in electronic payments, fraud detection has become increasingly important for financial institutions and their customers,” said Ralph Dangelmaier, president of the wholesale banking division at ACI Worldwide. “Bank account holders are becoming increasingly aware of common fraud schemes, and they want to be reassured that their information and assets are safe. By partnering with the industry's leading security companies, ACI is able to bring the power of aggregate volume pricing to our customers while providing them with industry-leading, integrated security solutions.”

Enterprise Banker is the first online banking application to launch a financial institution on the RSA Go ID authentication service network. When users login to Enterprise Banker, they are prompted for their unique one-time password token code before they are granted access to the application, or prior to releasing a payment. RSA Go ID hardware- and browser-based tokens provide users with a unique numeric password that changes every 60 seconds and can never be reused. The RSA Go ID toolbar is also engineered to include built-in phishing and man-in-the-middle protection – the toolbar will not permit a user to disclose his token-code at any site that's not pre-approved by the financial institution.

ACI customer FirstMerit Bank is now live on Enterprise Banker with the integrated RSA Go ID hardware token solution. “FirstMerit Bank of Akron was able to roll out 4,000 tokens in less than two weeks, with a user-friendly self-registration process,” said Stephen Mysko, senior vice president, treasury management, FirstMerit Bank of Akron. Two weeks later Enterprise Banker again was the first online banking application to launch Ocean Bank of Miami with the RSA Go ID toolbar token.

“We are delighted to have ACI Worldwide as a valued strategic partner that has led the market as the first to launch RSA Go ID live,” said Christopher Young, vice president and general manager, Consumer Solutions at RSA. “The RSA Go ID Network is gaining great momentum in the market. The various authentication options, such as hardware devices and the toolbar, as well as its streamlined fulfillment process and easy integration with our risk-based authentication technology make it a compelling solution for financial institutions. We look forward to further expanding the RSA Go ID Network in 2007.”

Additionally, ACI has 14 banks deploying Enterprise Banker with RSA's risk-based authentication technology at application logon. According to RSA's recent Financial Institution Consumer Online Fraud Survey, 73 percent of account holders said they would like their financial institution to use risk-based authentication, and 69 percent believe financial institutions should replace username-and-password login with stronger authentication for online banking.

RSA Adaptive Authentication is designed to provide robust security with minimal impact on the user experience. With ACI's integrated risk-based authentication technology from RSA, financial institutions will immediately be able to conduct a behind-the-scenes assessment of the user's identity based on factors including log-on location, IP address, device information and transaction behaviour – which is augmented with out-of-band phone calls or secret questions for login transactions that are deemed high-risk. Customers that select the RSA technology also benefit from membership in the RSA eFraudNetworkSM community, which provides the financial institution with valuable fraud information - not only from their client base, but from all members of the network in real-time. This means the institution can protect itself from fraudsters.

“ACI Worldwide and TriCipher offer financial institutions world-class solutions in a tightly integrated package,” said Vatsal Sonecha, vice president, strategy and business development, TriCipher.

### About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance. RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities,

the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

#### **About TriCipher, Inc.**

TriCipher, Inc. provides Future Proof Risk Based Authentication. The TriCipher Armored Credential System™ (TACS) is the first authentication system that enables companies to deploy and manage multiple types of credentials from a single infrastructure. Through this flexible "Authentication Ladder," TriCipher delivers future-proof security — protecting customers' investment by enabling authentication strength to adjust in response to new threats and regulatory changes without the need to implement a new infrastructure. In addition, TriCipher delivers risk-based authentication, preventing online fraud through seamless integration with fraud detection systems, secondary authentication systems, and the ability to enforce security software presence checks for malware protection. Founded in 2000, TriCipher is headquartered in San Mateo, California. The company was incubated as NSD Security before launching as a separate entity in 2005 with backing from ArrowPath Venture Capital, Intel Capital, Trident Capital, and Wasatch Venture Partners. For more information, visit TriCipher on the web at [www.tricipher.com](http://www.tricipher.com).

#### **About ACI Worldwide**

Every second of every day, ACI solutions are at work processing electronic payments, managing risk, automating back office systems and providing application infrastructure services. Founded in 1975, ACI is a leading international provider of solutions for retail banking, wholesale banking and cross-industry systems. ACI serves more than 800 customers in 83 countries including many of the world's largest financial institutions, retailers and payment processors. Visit ACI Worldwide on the Internet at [www.aciworldwide.com](http://www.aciworldwide.com).

RSA, GoID and eFraudNetwork are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other products and/or services mentioned are trademarks of their respective companies.

Any statements in this press release regarding projected results are preliminary and "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995. In addition, this press release may contain other forward-looking statements including statements regarding Transaction Systems Architects, Inc.'s ("TSA"), its subsidiaries or third parties' expectations, predictions, views, opportunities, plans, strategies, beliefs, and statements of similar effect. The forward-looking statements in this press release are subject to a variety of risks and uncertainties. Actual results could differ materially.

For a detailed discussion of these and other risk factors, interested parties should review the Company's filings with the Securities and Exchange Commission, including the Company's Form 10-K filed on December 14, 2005, the Company's Form 10Q filed on February 9, 2006, the Company's Form 10Q filed on May 10, 2006, and the Company's Form 10Q filed on August 9, 2006.