



## RSA Secure Customer Identities and Assets: A Solution for Complying with the FACTA Red Flag Guidelines

According to the Federal Trade Commission (FTC), an identity is stolen every 4 seconds. In addition, identity theft topped the list of consumer fraud complaints filed with the FTC in 2007. Such alarming statistics have prompted 6 U.S. Federal agencies to enact the FACTA Red Flag guidelines requiring U.S. financial institutions and creditors to develop and implement a preventative program to mitigate the risk of identity theft for both new and existing accounts.

Helping organizations comply with the FACTA Red Flag guidelines is a core part of RSA's Identity Assurance strategy—the set of capabilities and methodology that minimizes the business risk associated with identity impersonation and inappropriate account use. Specifically, the RSA Secure Customer Identities and Assets solution offers a comprehensive portfolio designed to mitigate the risk of identity theft and fraud, instill customer confidence and help organizations comply with the FACTA Red Flag guidelines.

The RSA Secure Customer Identities and Assets solution is currently used to protect over 150 million online users across the globe. Many of the world's leading organizations, including nearly 50 of the Top 100 U.S. banks, 3 of the Top 10 retail service providers, and 3 of the Top 6 telecommunication companies use RSA's solutions to protect their customers across multiple channels. Our portfolio offers:

- Knowledge-based authentication for verifying user identities for new account origination and enrollment.

- Risk-based authentication for assuring user identities as they attempt to access sensitive account information.
- Anti-phishing services to help protect consumers who may have provided personal information to fraudulent websites.
- Transaction monitoring to monitor accounts for suspicious activity that might precipitate identity theft.

---

### Verifying Identities

---

RSA Identity Verification is a knowledge-based authentication (KBA) platform that assures user identities in real-time. RSA Identity Verification presents a customer with a series of top of mind questions utilizing relevant facts on the individual obtained by scanning dozens of public record databases. With industry-leading speed and accuracy, RSA Identity Verification delivers a confirmation of identity within seconds, without requiring any prior relationship with the user.

RSA Identity Verification is fueled by RSA's Intelligent Questioning technology which logically develops correct and incorrect answers using actual consumer data in real-time. This instantaneous matching greatly improves user experience while reducing the ability for someone other than the genuine user to guess correct responses.

RSA Identity Verification also provides improved accuracy in authenticating users with the Identity Event Module. The Identity Event Module improves security by measuring the level of risk associated with an identity and allowing the configuration of the system to automatically adjust the



The Security Division of EMC



The FACTA Red Flag rules extend beyond just banks and include organizations such as medical providers, telecommunication companies, utility providers, automobile dealers, and non-bank lenders.

difficulty of the questions during the authentication process in order to meet the specific nature of the risk. Some of the identity events that are measured include:

- **Public record searches.** Suspicious access to a user's public record reports.
- **Identity velocity.** A high volume of activity associated with an individual at several businesses.
- **IP velocity.** Multiple authentication requests generated from the same IP (often a strong indicator of fraud).

---

## Assuring User Identities

RSA® Adaptive Authentication is a multi-channel authentication and fraud detection platform providing cost-effective protection for an entire user base. Adaptive Authentication provides strong and convenient protection by monitoring and authenticating user activities based on risk levels, institutional policies, and customer segmentation. Powered by RSA's risk-based authentication technology, Adaptive Authentication tracks over one hundred indicators to identify potential fraud including device identification, IP geo-location, and behavioral profiles. Each activity is assigned a unique risk score; the higher the score, the greater the likelihood is that an activity is fraudulent.

Adaptive Authentication offers behind-the-scenes monitoring that is invisible to the customer. When an activity is deemed to be high-risk, a customer is only then challenged to provide additional authentication. With low challenge rates and high completion rates, Adaptive Authentication offers strong protection and superior usability and is an ideal solution for mass consumer deployment.

---

## Preventing Phishing

RSA FraudAction<sup>SM</sup> Service is a proven service geared toward stopping and preventing phishing, pharming and Trojan attacks that target online users. FraudAction offers end-to-end fraud protection—including 24x7 monitoring and detection, real-time alerts and reporting, forensics and countermeasures, and site blocking and shutdown. The service is supported by RSA's exclusive Anti-Fraud Command Center (AFCC), one of the largest and most experienced team of fraud analysts in the industry. The AFCC has been responsible for shutting down over 80,000 phishing sites and reducing the average life span of an attack from 72 hours<sup>1</sup> to a median of just 5 hours.

---

## Monitoring Transactions

RSA Transaction Monitoring is a complete online fraud detection and management solution that allows financial institutions and creditors to monitor, detect and investigate online fraud. Powered by RSA's field-proven Risk Engine, the Transaction Monitoring solution analyzes and calculates a real-time risk score for every online activity and presents high-risk activities in a user-friendly case management system. Financial institutions that have implemented Transaction Monitoring have reported up to an 80% reduction in fraud.

<sup>1</sup> Source: Anti-Phishing Working Group (APWG)