



## Online Banking Multifactor Authentication

Due to a dramatic rise in online identity fraud, the Federal Financial Institutions Examination Council (FFIEC) issued a guidance in October, 2005, specifically calling for stronger authentication for online banking transactions. The directive stated that single-factor authentication used to identify online customers, such as a password or PIN, is inadequate for high risk transactions. Subsequently, the NCUA released a directive that all credit unions and banks will be required to adopt multi-factor identification for online financial transactions by the end of 2006. Multi-factor authentication requires an additional layer of security and requires at least a second or even a third form of identification. EPL has formed a partnership with RSA Security to deliver RSA's Adaptive Authentication solution in conjunction with EPL's CUe-Branch online banking product to comply with the requirements of this directive.

### RSA Adaptive Authentication

- Mature, risk-based authentication coupled with time-honored one-time-passwords delivers flexible, cost effective consumer authentication.
- Demonstrable low false positives mean minimal impact on user experience and customer support.
- Tangible one-time passwords mean increased customer trust and loyalty.

### "One Size Fits All" Doesn't Work Anymore

Different customer groups require different levels of security. Different types of transactions are riskier than others. Different segments of customers desire various forms of protection. Achieving the right balance of authentication security without compromising the user experience or the bottom line is no easy task. RSA® Adaptive Authentication provides cost-effective protection for your entire user base through two approaches, delivered through one integrated solution: risk-based and one-time password authentication.

**The risk-based authentication module** is a behind-the-scenes technology that is designed to score the level of risk associated with a given activity or transaction—like account logon, bill payment or transfers—in real time. If that activity exceeds a predetermined risk threshold the user is prompted for an additional authentication credential to validate his or her identity. Proven low false-positives rate translate to minimal impact on customer service and total cost of ownership.

**One-time password authentication** offers tangible, time-honored security for the segments of your user base who routinely engage in sufficiently risky activities or who feel better protected by physical security and will reward your institution for providing this through consolidation of assets increased willingness to transaction online.

### The only solution with a cross-bank fraud network and a proven real-time risk engine

- Enables invisible authentication
- Addresses emerging threats and preempts obsolescence through self-learning and adaptation
- Provides lowest impact on genuine users; highest fraud detection rate

### The only solution with multiple methods of authentication deployable today

- Allows matching authentication strength with transaction risk
- Provides choice in user experience to you and your customers

**"Scalable. Flexible. Future-proof. Cost-effective. Proven"**