

## Best Practice for Online Banking Security

Identity theft and fraud have become the leading global crimes of the 21st century with far-reaching national security, personal security, and economic and social consequences.

The October 2005 FFIEC guidance, which calls for improved online authentication and customer protection, is an overdue response to the rising tide of identity theft and financial fraud. The agencies are acknowledging the need for better online authentication in an ever-growing e-commerce economy, and recommending pro-active and continuous risk assessment and mitigation by financial institutions.

With credit unions being asked by their members to take a more proactive approach to protecting their online banking security, responsibility is shifting from the back office to the front office and even up to the Marketing Department. More than ever, it is critical for credit unions to rebuild confidence in their online channel. The rise of awareness from members and acknowledgement from the FFIEC about security issues allows credit unions that employ best practices to differentiate themselves in their marketplace.

The FFIEC guidelines state that single factor authentication is not sufficient, and companies dealing with monetary transactions should implement *multi-factor authentication, layered security, or other controls* to improve customer protection.

The latest addition to our online risk management system is AccountLock™, an affordable two-factor solution that offers an immediate and long-term defense against unauthorized account access, while meeting the FFIEC guidelines. Even if a member is a victim of the ever-increasing phishing attacks, the stolen login ID/Password information is rendered useless unless the fraudster has access to the victim's physical computer. Our two-way authentication process also allows the member to recognize the credit union's true Website by pre-defining names for their computer.

By allowing a PC or laptop to become the second factor of authentication, there is no need for intrusive or expensive hardware tokens. If someone tries to access a member's account from an unknown device, we can alert the member via their preferred method: e-mail, SMS, or a phone call. We can even provide your members with the ability to take complete control over which computers are allowed to access their accounts.



At iovation, our approach is both open and modular. Credit unions can choose just baseline authentication with AccountLock™ or they can take it a step further and integrate AccountLock™ with our global Device Reputation Authority™ that matches devices to accounts, while protecting the absolute privacy of account information. By employing this best practice approach, credit unions can share information across multiple industries and protect their members against known bad devices. In both scenarios, credit unions will confidently protect their members, assets, and reputation.



**Jon Karl** is Vice President of Marketing and Business Development and founder of iovation. Mr. Karl has 15 years of experience in the financial services, advertising and software industries. Mr. Karl served as Accounts Director and a key member of the management team at Edge Design and Advertising. During his tenure, Edge was one of the fastest-growing agencies in the Northwest and continues today as a regional force in high-technology marketing. For more information about iovation's products, visit [http://www.iovation.com/products\\_and\\_services/whitepapers.php](http://www.iovation.com/products_and_services/whitepapers.php) and request a copy of our whitepaper, *Strategies For Responding To FFIEC Internet Banking Authentication Guidance*.