

## *Securing the Credit Union from the Inside to the Outside*

It is well understood that all manner of attacks, fraud, ID theft attempts and cyber-crimes come from outside the credit union's perimeter. For the most part, credit unions have successfully addressed these complex outside threats, but have not as adequately dealt with insider threats. They could implement many layers of controls in an attempt to eliminate insider threats completely, however employee productivity would be negatively impacted. At the other extreme is unfettered access to data which would be equally as disastrous.

Complicating the inside security situation further is the third piece of the puzzle: member service. Members want expedient answers to their questions and their problems resolved quickly. These real world member service issues create tremendous pressures on employees to send and receive information and conduct transactions in a timely manner. Obviously a balance is needed - one that will generate an acceptable tradeoff between insider security and worker productivity.

Whether a member is served in the branch, online or via the call center, all interactions and transactions require a detailed audit trail. If the credit union has an integrated audit trail in place at every member touchpoint, then employees are not likely to be tempted for whatever reason to commit fraud. However, the manner in which this audit trail is implemented and administered is critical for both regular staff and IT Departments.

The key for all employees is that any solution that is implemented is consistent and integrated. Our approach at Indigo Identityware goes beyond a Single Sign-on (SSO). Our advanced software solutions encompass not only Enterprise SSO, but Strong Authentication, Workflow Management, and Secure Remote Access. Indigo's clients enjoy a fluid consistency in how they access their workstation, network, domain, applications and buildings (with proximity cards).

In the real world, employees need an intuitive methodology for accessing all of these different resources. When a system is intuitive, it will be widely accepted by workers and simultaneously it will dramatically reduce the IT Department's trouble tickets. Very few things are as easy to use as a biometric fingerprint reader - with a simple swipe of the finger a person can access their workstation and virtually all of their applications. If the credit union prefers proximity cards over biometrics, we can easily use cards and readers as well.

We have seen time and time again that more consistency equals more productivity. With strong authentication in place, you can securely address computer access, software application access and fast teller switching. Lost passwords become a thing of the past! We like to say that our software "knows who you are," plus it knows what you have been doing via its auditing capabilities. The end result is a winning combination of practicality, consistency, enhanced security, better productivity and ease of use.

**Thomas J. Rheineck**  
President & CEO



**Thomas J. Rheineck**

is President & CEO of Indigo Identityware and is an accomplished health-

care and technology executive with over 25 years of experience in diagnostic imaging and health-care information technology, including over a decade of management roles at each of GE HealthCare and Center for Diagnostic Imaging (CDI). He holds an MBA from the University of Chicago and has served as Chairman of Lamplighters International as well as a current member of the Board of Directors for Logic Information Systems and Cardiowrite, LLC. Indigo Identityware is a leader in the Identity and Access Management industry. Indigo distinguishes itself by offering the first and only Behavioral Strong Authentication and Single Sign-on (ESSO) for the extended enterprise.

### Contact Info

[www.indigoidentityware.com](http://www.indigoidentityware.com)