

Finding a Balance between Security and Convenience

To be truly effective, security must be a component of everything a bank does, not just an “add on.” It must be embedded in the way that the bank runs its operations, and be an integral part of its core philosophy. Effective security implies successful risk management. In fact, the first steps of any security project should always involve a risk assessment, followed by a plan to deliver effective controls of the documented risks and a permanent program to ensure the controls are continually evaluated.

Until recently, most every governmental regulation of a security nature was focused on the bank’s back office systems and personnel, in areas like firewalls, encryption and similar technology. These regulatory changes and decisions had little to no impact on customer experience. However, with the recent introduction of the FFIEC and FDIC strong authentication guidance, changes necessary to conform with compliance requirements have begun to have a direct impact on the end users of an online banking system. As the security process becomes a more important part of the relationship between the bank and its online customers, more and more people at the institution are becoming involved in the risk assessment and decision-making process. Not only are the IT and risk departments involved, but the Marketing Department, Call Center and other customer-facing departments are engaged, as well.

We recognize the fact that a significant number of customers may not be as concerned about online account security as the bank IT and security professionals who are tasked with protecting confidential customer information. With this in mind, Corillian designed our Intelligent Authentication™ application to be easy to use, implement, configure and maintain. For example, the bank may choose to allow customers to decide when they want to activate the strong authentication capability on their accounts, at a time that is convenient for the customer. This not only makes it more convenient for the customer, it also helps to create a true sense of ownership of the security process on the part of the customer due to the opt-in nature of the program. Once enrolled, users are only disrupted when absolutely necessary. Intelligent Authentication only challenges users when it detects access behavior that is inconsistent with the user’s past verified behavior (for example, if they visit from an unknown geographical location, at an unusual time of day, with a different browser or operating system, etc.). Challenges can take the form of secret questions and answers, telephone calls, or a variety of other flexible forms of authentication.

When we designed Intelligent Authentication, our goal was to make it as minimally disruptive as possible to customers, while still providing an effective and appropriate level of strong authentication to banks – and for the system to be flexible in configuration in order to match the bank’s risk tolerance requirements and needs. If the bank is happy with using challenge questions, that’s available; but if they want to use hardware tokens or out-of-band methods like authenticating via telephone, we support those as well. It all comes down to choice and flexibility – each bank has a different set of unique requirements and should have the option to pick and choose those security methods that best suite its particular needs.

At Corillian, our core competencies include building, running and securing high performance online banking systems for financial institutions of all sizes. So it was only natural for us to leverage our internal security methods and make them available to our hundreds of financial institution clients. For instance, the Corillian Fraud Detection System (CFDS) has been in use in our data centers for years and is now protecting many banks by detecting a variety of suspicious activity before it escalates into fraud, identity theft or other crimes. CFDS proactively analyzes suspicious behavior and produces reports for security and risk mitigation purposes. When combined with Intelligent Authentication, it makes for a powerful layered online defense system. A proactive, layered security posture that works for the users of your online system is important in today’s operating environment. As threats evolve and the landscape continues to change, ensuring you are partnered with companies that can help you do an excellent job of securing the many aspects of your environment is critical.



Greg Hughes
Chief Security Executive

Greg Hughes is Chief Security Executive and VP of Security and Information Technologies at Corillian. Hughes oversees the development and implementation of company-wide security principles, policies, and practices; leading the Corillian Security Solutions business unit, including the architecture and development of Corillian's security software products; and driving corporate IT planning and strategy. Hughes also has responsibility for the oversight and coordination of security activities related to Corporate Offices, Product Development, Professional Services, Hosting Services, Corporate Information Technologies, and Facilities. Prior to his current role, Hughes served as Director of the Security and Information Technologies divisions at Corillian. Hughes also worked in Corillian's Marketing and Communications department.

