Ensuring Safe Financial Transactions and Regulatory Compliance at Cornerstone Community Bank

AhnLab Online Security employed to protect sensitive customer data

Organization Overview

Cornerstone Community Bank

Cornerstone is a single-bank holding company with $426 million in assets that serves the Chattanooga, Tennessee MSA. Locally owned and locally operated, Cornerstone Community Bank (www.cscbank.com) was founded in 1996, and is one of Chattanooga's oldest and largest community banks.

With five branches serving the Hamilton County area and one loan production office in Dalton, Georgia, Cornerstone Community Bank specializes in providing a comprehensive range of customized financial solutions for businesses and individuals.

New Regulations for US Financial Institutions

"Layered Security" is a relatively new approach to online transaction security implemented by US financial institutions. In June of 2011, the Federal Financial Institutions Examination Council (FFIEC) and the Federal Deposit Insurance Corporation (FDIC) issued new guidelines for financial institutions to protect against theft of sensitive customer data. These new guidelines encourage financial institutions to implement layered security controls and address endpoint security.

US financial institutions, such as Cornerstone Community Bank (CCB) of Chattanooga, Tennessee, must meet these new guidelines in order to remain compliant with federal regulations and to ensure the integrity of their customers' online transactions. To accomplish these goals, CCB turned to a solution powered by AhnLab's Online Security (AOS).

Increased Protection Needed for Sensitive Data

Current authentication mechanisms used for online banking are vulnerable to security breaches. Single-factor authentication, in the form of a typical username and password login, does not provide sufficient protection to meet the new FFIEC/FDIC guidelines. Instead, financial institutions must implement multi-factor authentication, or layered security, and other controls to mitigate these risks.

According to the financial institution letter, FIL-50-2011: Supplement to Authentication in an Internet Banking Environment, US financial institutions are required to employ effective methods to authenticate customers' identities and these methods must mitigate the risks associated with the use of sensitive customer information.

The purpose of the FIL is to reinforce the risk-management framework described in the original guidance published in 2005 and to update FFIEC-member agencies' supervisor expectations regarding authentication and protection of data in an increasingly-hostile online environment. The supplement also establishes the new minimum standard against which banks are held legally accountable for claims resulting from leaked or compromised data.

More Protection Needed at Endpoints

In FIL-50-2011, the requirements for authenticating financial transactions include three main areas of control: initiation (endpoints), transmission, and the back office. A detection process must respond to any

suspicious activity at initial login and at initiation of a transfer of funds. When responding to the 2005 guidance, many financial institutions implemented simple device identification measures that consisted of loading cookies onto customer endpoints.

However, experience since that time has shown that these cookies can be surreptitiously copied or relocated to fraudulent systems to allow hackers to impersonate customers. The new guidance outlines increased security for endpoints as a prime part of the new responsibilities for financial institutions.

Ensuring Compliance at Cornerstone Community Bank

CCB began evaluating their security architecture and approaches as soon as FIL-50-2011 was released. According to Kimberly Adams, the Vice-President and Information Security Officer at Cornerstone, the bank had strong controls in place and a certificate-based endpoint solution that might technically meet the new regulations. But, as she stated, "we needed to do more on the endpoint authentication and transaction security for our commercial Automated Clearing House (ACH) and Remote Deposit Capture (RDC) clients."

Together with the Vice-President of Information Technology, Randy Dover, Adams defined the design of a solution that would ensure the integrity of their client endpoints:

> *"First and foremost, the solution had to address current and potential security threats from endpoints… Next, the solution had to fit within our Information Technology infrastructure by way of footprint and support requirements. Finally, we had to have a solution that was easy for our non-technical clients to adopt."*

Evaluating an AhnLab-powered Solution

CCB's requirements involved separating web sessions from the executing device, so that malware at endpoints could be isolated. They found several non-affiliated vendors who could piece together partial solutions, but it was a joint solution offered by AhnLab and SafeNet that created a "trusted browsing" environment, providing a fresh, convenient approach to endpoint security that offers secure access to online banking applications and identity protection on a USB token.

The AhnLab-SafeNet Trusted Browsing Platform combines the strength of AhnLab Online Security

"AOS gave us reasonable confidence that malware located on an endpoint could not interfere with our certificate-based authentication and integrity of the financial transaction."

Kimberly Adams, Vice-President and Information Security Officer, CCB

Secure Browser and Anti-Keylogger features with SafeNet's certificate-based eToken NG-FLASH Anywhere USB authenticator. AhnLab Secure Browser with eToken NG-FLASH Anywhere creates a portable, zero-footprint USB flash device with a built-in hardened web browser that runs from the read-only memory drive of the device, restoring trust to the browser application and preventing MITB attacks from occurring. It offers a secure access solution that goes where you go, so banking customers can access web applications from anywhere, without worry. The Trusted Browsing Platform offers dual protection by using certificate based strong authentication to validate the identity of the customer at logon and by preventing memory hacking, webpage alteration, SQL injection, cross-site scripting (XSS), browser help object (BHO) hacking, screen capturing, debugging, and reverse engineering. The Anti-Keylogger also protects sensitive personal data entered via a keyboard.

CCB compared the Trusted Browser approach to an "out-of-band" phone solution that was combined with a secure browser server. They discussed the strengths and disadvantages of each solution and decided that the USB key approach was superior for multiple reasons. As Adams explains,

> *"The SafeNet/AhnLab solution would be easier for our clients to adopt and for us to implement and maintain… [It] didn't have much of an IT footprint and really required minimal IT resource investment to configure and maintain. We don't have to worry about maintaining new business-critical server software or keeping up with client phone numbers. All in all, we found the SafeNet/AhnLab solution to have less moving parts that could break."*

Satisfied Requirements, Satisfied Customers

When clients plug SafeNet's eToken NG-FLASH Anywhere token with the onboard AOS Secure Browser and AOS Anti-Keylogger into their endpoints, Cornerstone Community Bank's secure web session starts automatically. The security-heavy work is performed in the background and clients see the CCB login screen, just as if nothing had changed. When they remove the SafeNet token, the session is automatically closed, leaving no footprint. For CCB's clients, immediate protection is provided with no installation or learning curve required.

AhnLab and SafeNet's Trusted Browsing solution provides identity protection and wards off hacking attempts, Man-in-the-Browser (MITB) attacks, and Man-in-the-Middle (MITM) attacks. It offers a

"The…software allows you to insulate the authentication and transaction from threats. On top of that, it is easy for the client to adopt, which is a bonus."

*Kimberly Adams, Vice-President and Information Security Officer, **CCB***

secure, portable, device-independent solution that allows CCB's customers to perform banking transaction anywhere, without having to worry about their sensitive data. Adams and CCB's team are pleased that the Trusted Browsing Platform has allowed them to ensure regulatory compliance and better serve their customers, while meeting their project goals: "By adopting the SafeNet's solution with the AhnLab Secure Browser and Anti-Keylogger, we have accomplished our goals: (1) fortify commercial client with financial integrity at the endpoint, and (2) ease of client adoption."

AhnLab Online Security is in collaboration with SafeNet eToken NG-FLASH Anywhere

SafeNet is a leading global provider of data protection. For over 25 years, Fortune 500 global corporations and government agencies have turned to SafeNet to secure and protect their most valuable data assets and intellectual property.

About AhnLab

AhnLab develops industry-leading information security solutions and services for consumers, enterprises, and small and medium businesses worldwide. As a leading innovator in the information security arena since 1995, AhnLab's cutting-edge technologies and services meet today's dynamic security requirements, ensure business continuity for our clients, and contribute to a safe computing environment for all.

We deliver a comprehensive security lineup, including proven, world-class antivirus products for desktops and servers, mobile security products, online transaction security products, network security appliances, and consulting services.

AhnLab has firmly established its market position and manages sales partners in many countries worldwide.

AhnLab, Inc.
www.ahnlab.com
global.sales@ahnlab.com
Tel: 1-888-537-4336

673, Sampyeong-dong, Bundang-gu,
Seongnam-si, Gyeonggi-do,
463-400, Korea

AhnLab