



April 29, 2002

Secretary  
Federal Trade Commission  
Room 159  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

Re: Public Workshop: Consumer Information Security  
67 FR 10213 (March 6, 2002)

Dear Sir or Madam:

America's Community Bankers ("ACB")<sup>1</sup> is pleased to comment on the proposal regarding security issues facing businesses that maintain consumers' personal information.<sup>2</sup> These comments are being provided prior to the Federal Trade Commission's public workshop on consumer information security.

Community bankers actively protect customer information. ACB members have gone beyond comprehensive regulatory requirements and have developed proactive strategies that protect customer information and preserve customer trust.

**Customers Expect Community Banks to Actively Protect Personal Information**

ACB members have an outstanding record of protecting the confidentiality and security of customer information. Because consumer trust is one of the cornerstones of a community bank's business relationships, these institutions will continue to protect the confidentiality of consumer information as part of their business practices. Community banks compete with non-banks that offer similar products in today's fast moving and increasingly competitive financial marketplace; the trust they have earned provides them with a key competitive edge.

---

<sup>1</sup> ACB represents the nation's community banks of all charter types and sizes. ACB members, whose aggregate assets exceed \$1 trillion, pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

<sup>2</sup> 67 Fed. Reg. 13767 (Mar. 26, 2002).

Secure facilities, safes, alarm systems, dual control procedures and trustworthy employees have been the traditional mechanisms used to protect banks and their assets. However, the exploitation of technology is a significant risk to banks and their customers. All banks are challenged to provide exceptional service and meet increased consumer demand for Internet banking services, while maintaining the security of customer information. Every Internet-connected bank is vulnerable to electronic threats; however, community banks adhere to federal regulations for safeguarding customer information and proactively implement additional security measures to defend against internal and external attacks.

**Community Banks Protect Customer Information By Following Comprehensive Regulatory Requirements.**

The Gramm-Leach-Bliley Act requires all financial institutions to “safeguard and protect confidential information by adhering to joint guidelines issued by the federal banking agencies.”<sup>3</sup> These standards, known as *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*,<sup>4</sup> require banks to establish administrative, technical, and physical information safeguards. They are designed to:

1. Ensure the security and confidentiality of customer records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of such records; and
3. Protect against unauthorized access to or the use of such records or information that could result in substantial harm or inconvenience to any customer.

The Guidelines require all financial institutions to implement a comprehensive written information security program that is appropriate to the size and complexity of the bank and the nature and scope of its activities. The information security program must include a written policy and operational procedures that protect confidential customer information and bank proprietary information. The information security program must:

- **Involve board of directors.** The board must approve the written information security program and must oversee efforts to develop, implement, and maintain it.
- **Assess the sensitivity of customer information.** Banks must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information (i.e. inadvertent disclosures, theft by an outsider, theft by an

---

<sup>3</sup> 15 USC 6801(b), 6805(b). The federal banking agencies include the Federal Deposit Insurance Corporation (“FDIC”) the Federal Reserve Board, the Office of the Comptroller of the Currency (“OCC”) and the Office of Thrift Supervision (“OTS”).

<sup>4</sup> 12 CFR Part 30 (OCC); 12 CFR parts 208, 211, 225, and 263 (Federal Reserve); 12 CFR 364 (FDIC); 12 CFR Part 570 (OTS).

insider, pretext calling, etc.) Each bank must also assess the sufficiency of existing policies, procedures, customer information systems, and other arrangements that are intended to control the risks it has identified.

- **Take steps to manage and control the risks identified.** Banks must design information security programs to control identified risks, commensurate with the sensitivity of customer information and the complexity and scope of the bank's activities. Once a security program has been developed, staff must be trained to implement it. The program's systems and key controls must be regularly tested.
- **Oversee service provider arrangements.** Banks must exercise appropriate due diligence in selecting service providers and by contract must require service providers to meet the objectives of the agency guidelines. After contracting, banks must monitor the service provider's performance by reviewing audits and summaries of test results.
- **Adjust the program.** Banks must "monitor, evaluate, and adjust" their information security program as circumstances change within the institution. Mergers and acquisitions as well as modifications in business arrangements, technology, outsourcing, or changes in the sensitivity of customer information warrant adjustment of the information security program.
- **Report to the board of directors.** On an annual basis, each bank must report the information security program's overall status and the bank's compliance with the Agency guidelines. This presentation should discuss risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations, and management's responses and recommendations for changes in the information security program.

**Community Banks Proactively Defend Customer Information From Internal and External Threats.**

**ACB Network Security Study**

In recognition of a growing concern among ACB members regarding Internet security and related regulatory requirements, ACB worked with SecurePipe, Inc. to survey network security risks faced by ACB member banks. The study, based on a representative sample of ACB membership, was designed to take a brief but detailed "snapshot" that would provide bankers with insights about the general nature of Internet security in community banking.

Like all businesses connected to the Internet, every network was susceptible to the proliferation of viruses and automated hacking programs. Virus attack signatures were detected on every network analyzed, which serves as a stark reminder of the relentless virus threat.

A majority of the networks analyzed detected attempts to scan the bank's network. Network scans and automated attack attempts are driven largely by automated processes that scan large blocks of network address space looking for available victims. A bank is not isolated from the threat posed by this activity because it does not engage in e-banking; the threat is simply the function of having an Internet connection.

The SecurePipe study effectively illustrates the vulnerability of all Internet connected businesses. To combat these unseen foes, community banks go beyond regulatory guidelines and have developed a proactive strategy for implementing a variety of security measures to protect customer information and customer trust. Because the financial success of community banks depends on the continuing integrity of their systems, these institutions combine internal risk management, expert advice, periodic testing, systems analysis, and threat monitoring to provide an effective defense. Community banks also:

- Deploy anti-virus systems that cover e-mail, web browsing, and file transfer or sharing;
- Utilize fire walls to limit their exposure to outside attacks;
- Encrypt customer information;
- Place access controls on customer information systems;
- Exercise dual control procedures, segregate duties, and conduct employee background checks for employees with access to customer information; and
- Detail actions that must be taken if the bank suspects or detects that unauthorized individuals have gained access to customer information.

### **Identity Theft Prevention and Aid**

Identity theft, the nation's fastest growing crime, is costly to banks and consumers. Because customer education is key to combating this growing fraud, ACB has developed two statement stuffers banks can offer their customers that expose common identity theft scams and offer tips to consumers on protecting themselves. Copies of these statement stuffers are attached to this letter. Some ACB members are employing technology to help combat identity theft. For example, several members use sophisticated transaction profiling systems that identify fraudulent transactions by searching for activities that are inconsistent with a customer's usual transaction patterns. Other community bankers have compiled a resource guide for customer support personnel to use when assisting identity theft victims.

### **Conclusion**

ACB appreciates the opportunity to comment on this important matter and supports the FTC's effort to facilitate a discussion of the protection of customer information. If you


Consumer Information Security

April 29, 2002

Page 5

have any questions, please contact the undersigned at (202) 857-3121 or via email at [cbahin@acbankers.org](mailto:cbahin@acbankers.org); or Krista Shonk at (202) 857-3187 or via email at [kshonk@acbankers.org](mailto:kshonk@acbankers.org).

Sincerely,

A handwritten signature in cursive script that reads "Charlotte M. Bahin". The signature is written in black ink and is positioned above the printed name and title.

Charlotte M. Bahin

Director of Regulatory Affairs, Senior Regulatory Counsel