Testimony of
America's Community Bankers
on

"H.R. 3997, the Financial Data Protection Act of 2005"

before the

Subcommittee on Financial Institutions
and Consumer Credit

of the

Financial Services Committee

of the

United States House of Representatives

on
November 9, 2005

Josie Callari
Senior Vice President
Astoria Federal Savings
Lake Success, NY
and
Vice Chairman
ACB Electronic Banking and Payment Systems Committee

Chairman Bachus, Ranking Member Sanders, and members of the committee. My name is Josie Callari, and I am testifying today on behalf of America's Community Bankers.[1] I am Senior Vice President of Astoria Federal Savings, headquartered in Lake Success, New York. Astoria Federal Savings is a full service financial institution providing retail banking services to the New York City area, and home financing to 14 states. I have 30 years experience in the banking industry, ranging from my start in a retail branch to my current position as Director of Banking Operations at Astoria Federal Savings, with a staff in excess of 200. In addition to my duties at Astoria Federal Savings, I serve as Vice Chairman of ACB's Electronic Banking and Payments Committee.

ACB appreciates having the opportunity to testify before the Subcommittee on H.R. 3997, the Financial Data Protection Act. The issue of data security is critical for community banks. The number of high-profile data breaches that occurred this year brought to light possible vulnerabilities that have been created due to the Internet revolution. While banks have had the mandate to safeguard sensitive customer information for years, the growth of the Internet and electronic commerce has made compiling and selling sensitive personal information easier for a multitude of companies, creating a need for comprehensive data security legislation.

That is why ACB supports H.R. 3997, introduced by Congressmen LaTourette, Hooley, Castle, Pryce, and Moore. This legislation is a common sense approach to providing a meaningful solution. Identity theft and account fraud are real and growing crimes in the United States, and the expanding amount of consumer information that is collected and stored by businesses has the potential to feed the identity theft problem. This country needs legislation that addresses the problem, not the symptom. That means focusing on stopping the misuse of consumer information, and creating an incentive for companies to make securing customer data a priority. Mr. Chairman, ACB believes that H.R. 3997 achieves this goal in a way that protects consumers, helps to prevent the abuse of consumer information, and gives companies an incentive to do the right thing, while maintaining maximum flexibility for all types of businesses.

Review of H.R. 3997

Let me start discussing ACB's view on H.R. 3997 by giving a background of ACB's principles for all data security legislation. Earlier this year ACB's board of directors laid out its top priorities for any data security legislation that may be considered in Congress. These priorities included:

1) Creating a national standard
2) Exempting institutions subject to existing GLBA data security requirements
3) Maintaining functional regulation
4) Providing fullreimbursement of costs by those responsible for security breaches

[1] America's Community Bankers is the member-driven national trade association representing community banks that pursue progressive, entrepreneurial and service-oriented strategies to benefit their customers and communities. To learn more about ACB, visit *www.AmericasCommunityBankers.com.*

ACB is pleased to see that H.R. 3997 addresses our top three priorities, and that it begins to deal with the difficult issue of reimbursement.

National Standard

Having a national standard is critical for any legislation addressing data security and consumer notices. Adding another layer of regulation to a rapidly growing patchwork of state and local laws hurts consumers, hurts the economy, and will not provide effective protection. Our nation's economy has evolved to the point where commerce and banking are nationwide activities. People can travel anywhere in our country at any time, and thanks to the Internet, conduct business throughout the nation from the comfort of their home. When it comes to the nation's payment systems, borders mean little. A balkanized patchwork of state laws that provide protections that stop and start at state lines will not provide meanful protection for consumers in a national marketplace. Over 40 million Americans move every year, and they expect to have the same protection of sensitive personal information in their new home as they did in their old. Having a uniform national standard for data security and breach notices will afford them that protection. Furthermore, consumer information should be protected equally regardless of the state where the transaction occurred. Consumers deserve uniform protection, and ACB believes that the Congress has an obligation to provide it.

Gramm-Leach-Bliley Exemption

Additionally, ACB believes that Congress should recognize that the Gramm-Leach-Bliley Act (GLBA) already requires financial services companies to have in place much of what is being considered in most data security legislation. Title V of GLBA requires financial services companies to implement data security safeguards, a customer response program, and a comprehensive privacy policy. This spring the banking regulators issued guidance extending Title V to require customer notices in case of a breach that puts consumers at risk. To layer a duplicative regulatory system on top of this robust framework would only increase costs for financial institutions, and ultimately their customers. Such a system is unnecessary and ultimately would be harmful.

In addition, ACB applauds the committee for requiring that regulators work to harmonize existing GLBA standards to the greatest extent possible with those that will be required for non-financial institutions. Consumers should not experience different protection for their sensitive information based on what type of company they do business with. However, I urge that the committee work to ensure that any new rules do not place unnecessary burdens on financial institutions, and recognizes that they do have some unique needs and requirements.

Functional Regulation

Likewise, financial institutions have an incredibly robust regulatory framework under which they operate. This is particularly true for depository institutions. The banking regulators regularly examine financial institutions to ensure safety and soundness and consumer protection. ACB applauds H.R. 3997 for embracing this existing framework by vesting enforcement with functional regulators. This will result in both a more efficient regulatory structure and more

uniform consumer protections. Some have contemplated a system where enforcement would be vested with various state entities, such as state Attorneys' General. This would lead to uneven enforcement, where enforcement might depend on arbitrary local considerations rather than a uniform, predictable approach to national enforcement. As a banker I have grave concerns about such a system because it could infringe upon the principles of the dual chartering system for financial institutions. As I said earlier, the protection of a person's sensitive personal information should not depend on where they live or where a particular company is located. This is unfair for consumers. We need uniform enforcement, and vesting enforcement with established agencies of national scope and responsibility achieves that goal in an efficient and reliable manner.

Other Important Provisions

I also would like to highlight some of the other parts of H.R. 3997 that ACB supports. One of the most difficult aspects of crafting legislation to prevent the misuse of consumer information is creating a trigger that will notify consumers when they are at risk for fraud or identity theft, but not inundate them with unnecessary notices that cause unnecessary concern and ultimately desensitize consumers. By using a standard of "reasonably likely" to cause harm, the legislation has struck a good balance between the need to notify and the objective of providing meaningful notices. Additionally, ACB applauds the committee for recognizing the difference between account fraud and identity theft. These two distinct problems have often become blurred as one in popular debate, but for consumers there is a distinct difference between the two risks. Transaction fraud poses minimal risk to consumers because they have no liability for fraudulent credit or debit card transactions, and regulations specify standards for speedy resolution. Transaction fraud generally creates only a temporary inconvenience. However, identity theft can be much more harmful for consumers, and they must take concrete steps to prevent identity theft as quickly as possible if they are at risk. The dual notices recognize these differences and provides consumers with the appropriate information to address the risk.

Finally, ACB supports efforts to ensure that banks have the ability to be part of an investigation into possible breaches. The requirement for joint investigations between companies and their third parties helps to ensure that community banks will not be left in the dark when an investigation is ongoing. Furthermore, requiring that contracts between companies and their third parties address who is responsible for sending notices is very important. Many community banks believe they should be the ones to send breach notices to their customers, regardless of who is responsible for the breach. Community banks are proud of the relationships they have with their customers, and generally would prefer be responsible for sending a breach notice, rather than what is likely to be an unknown company communicating with the bank's customers.

Potential Area of Concern with H.R. 3997

As I mentioned before, ACB supports H.R. 3997, and hopes to see the committee act quickly on it. However, there are two areas where ACB's members have concerns, and we look forward to working with the committee and the bill's sponsors to address these concerns. First and foremost, ACB believes that those who are responsible for a data breach must be responsible

for the costs of protecting consumers from risks arising from the breach. The committee has taken the first step towards this by requiring that the party responsible for the breach should bear the cost of sending notices. This is common sense, but notices are only a small part of the cost of protecting consumers. One of the biggest costs is that of reissuing credit and debit cards, and closing accounts placed at risk. ACB's members have estimated that the replacing cards can cost up to $15. In instances where a community bank has thousands of cards affected these costs can mount quickly, and the institution ends up bearing all of the costs itself. Community banks are doing this now because they are dedicated to protecting their customers, however, they should not have to bear those costs. Those responsible for the breach should bear them.

Finally, ACB's members have expressed concern that there is no limit on how long an investigation required under a bill can take. Our members support the structure requiring investigations, which allow companies a chance to assess the severity of a potential breach, and the risk it poses to consumers. This is a responsible approach and allows companies the flexibility they need to protect consumers. However, ACB's members are concerned that without guidance the investigations could take an excessively long time, leaving consumers at risk. We believe that it is not advisable to legislate hard deadlines for investigations because each one is unique and will require a different response. However, the bill should require that as part of the overall rulemakings, regulators should give guidance on the appropriate length of an investigation.

Conclusion

In conclusion, ACB supports H.R. 3997 and urges the committee to consider it soon so that consumers can enjoy the protections it would provide. ACB urges that H.R. 3997 be passed with constructive modifications such as those suggested, but without adding provisions that take the bill's focus away from securing consumer data, providing appropriate and timely notices, and creating the right incentive structure and enforcement mechanism to stop the misuse of consumer information. This bill is crafted to be workable and effective, but adding provisions unrelated to its core purpose could jeopardize its potential benefits. We look forward to working with you as the committee crafts legislation that best addresses the problems of data security breaches.