Photograph by Patrick T. Fallon/Bloomberg

Any corporate scandal reaches a stage at which all affected parties descend on Washington for a rousing round of finger-pointing. That time has come in the debate over consumer data security that was set off in December when hackers accessed the personal information of up to 110 million Target (TGT) customers.

A top Target executive, federal regulators, and trade groups for stores and banks will testify at a series of hearings throughout the week as lawmakers consider what they can do to keep our credit-card and social security numbers from being stolen and auctioned to the highest bidders. A major dynamic will be the retail and financial industries assigning blame to one another. The theme of shared responsibility features prominently in prepared testimony submitted in advance by representatives from industry groups. While at first glance this can sound like a kumbaya moment, it's also a polite way of saying that other folks haven't been holding up their ends of the bargain.

James Reuter, an executive vice president from FirstBank (FBMI) speaking on behalf of the American Bankers Association, noted that banks have borne over 60 percent of reported fraud losses, even though they have accounted for fewer than 8 percent of reported breaches since 2005. "When a retailer like Target speaks of its customers having 'zero liability' from fraudulent transactions, it is because our nation's banks are making customers whole, not the retailer than suffered the breach," he argued in testimony submitted on Monday to a Senate Banking Committee panel.

Story: Why the U.S. Leaves Its Credit-Card System Vulnerable to Fraud

The banks want retailers and other companies holding financial data to be held to the same data-protection standards as bankers. Already, 46 states have some sort of standard for how companies that have suffered breaches must tell their customers, but banks want a federal standard as well, and senators Roy Blunt (R-Mo.) and Tom Carper (D-Md.) have introduced a bill that would create one. Reuter also says that banks shouldn't be footing the bill when other companies are to blame. "When any entity—be it a bank, merchant, college or hospital—is responsible for a breach that compromises the customer payment data or personally identifiable information, that entity should be responsible for the range of costs associated with that breach to the extent it was not adhering to the necessary security requirements," he said.

When representatives of the retail industry talk about sharing responsibility, they're talking about a suddenly infamous characteristic of U.S. credit cards: the use of magnetic strips, instead of the computerized chips that many other countries use. They say they've been forced into insecure practices. "For years, retailers have urged banks and card networks to adopt the enhanced fraud prevention technology (PDF) in use around the world here in the United States. While their resistance to doing so has been great, retailers continue to press all other stakeholders in the payments system to this a priority," argued William Hughes of the Retail Industry Leaders Association in a letter sent to the panel.

While the failure to adopt computer-chip technology didn't directly lead to the Target breach, magnetic strips are easily counterfeited, making U.S. consumer information more valuable than similar information about people living in countries that use harder-to-spoof chip cards. Pretty much everyone agrees that the U.S. needs to do this, and a major deadline for adoption is slated for next year. Even in the best-case scenario, the credit-card industry will continue to rely, at least somewhat, on magnetic-strip cards for at least a decade, says David Robertson, publisher of the *Nilson Report*, an industry newsletter.

Story: Canadians Didn't Trust Target Even Before the Data Breach

Some of the most valuable information acquired about Target's customers was not their credit-card numbers but further personal information whose loss was disclosed weeks after the initial revelations. This data, which included such items as phone numbers and e-mail addresses, can be used for more sophisticated identity theft schemes in which criminals open phony accounts in customers' names, as opposed to credit cards mostly used to run up fraudulent charges in the short term. This has little to do what kind of credit card gets swiped.

It's not clear what exactly the federal government can do on data security, and there's a fair amount of skepticism that it can figure anything out this week. "Maybe the politicians are going to raise a ruckus, get some headlines, and do nothing," says Robertson. "That would be likely." Edmund Mierzwinski, the consumer program director of the U.S. Public Interest Research Group, raises a more fundamental question: Does a company like Target really needs

to collect a full dossier on its consumers in the first place? “Congress should investigate the over-collection of consumer information for marketing purposes,” he said in prepared testimony. “More information means more information at risk of identity theft.”

Story: Hewlett-Packard Depresses Us Some More on the State of Cybersecurity
Brustein is a writer for Businessweek.com in New York.