Consumers Union
Nonprofit Publisher of Consumer Reports

Here's What's at Stake in the Congressional Debate About Data Security Breach Notice:

Consumers Union says that consumers should get notice of each breach which reaches, or is reasonably believed to have reached, the consumer's personal identifying information, such as social security number, account number, drivers license number, credit card or debit card number, and similar information.

- Notice will not be required if a hacking or lost data incident does not include specific personal information.

- In all other cases, notice should be required, with no special exceptions for particular industries.

The company that had the security breach should not be allowed to decide whether or not to give the notice.

Entities that hold our data say that consumers shouldn't be flooded with notices. They propose that notice of a security breach should be required only if there is a risk of harm to consumers.

Here's what this argument doesn't consider:

- Any standard that hinges on a determination of likely risk of harm means that consumers get no notice when no one knows who took the data, or why.

- Information can be taken from a data broker, retailer, or bank and used with a different entity to open a new credit account. The business whose security was breached has no way to know how the information is, or might be, used with someone else.

- After the loss of a back up tape reported to contain more than three million unencrypted names and social security numbers, CitiFinancial still claimed that "there is little risk" to consumers.

- A harm trigger leaves the burden of uncertainty on the consumer: Any trigger that requires a risk of harm may leave consumers in the dark when the breached company doesn't know who intruded into their data system, or why the intruder acted. A company might argue that it can't conclude or know that there is a risk of harm if it doesn't know the identity or purpose of the intruder. If the company doesn't know who breached the system or stole the laptop or the back-up tape, it can claim that it doesn't know whether or not consumers are at risk. Any standard that ties notice to knowledge of a risk of harm leaves consumers with no notice in the event of incomplete facts about the data security breach.

- A harm trigger that the breached entity applies lets the company with an interest in keeping the data breach secret be the one who decides if notice is required. This is an inherent conflict of interest.

- When businesses know that they must tell consumers about every security breach that reaches certain personal information, they may choose to invest more in data security, preventing more breaches. Thus, a strong notice law can protect consumers partly by encouraging better security, which reduces the number of breaches and thus the number of notices.

- Consumers need to know *every* time an unauthorized person has accessed his or her personal identifying information, such as last name, address or phone number plus a social security number, driver's license number, or account number. This information is enough to open new credit accounts.

- Information can be taken from a data broker, retailer, or bank and used with a different entity to open a new credit account. The entity who had the security breach has no way to know if the stolen information is, or might be, used with someone else. [1]

Some are asking Congress to eliminate state laws requiring notice of breach or other consumer protections:

Here is what this request overlooks:

- Consumers probably still wouldn't know about the 50 million persons affected by data breaches in 2005 if not for the California law, which required ChoicePoint to notify Californians, and the efforts of 38 state Attorneys General to encourage notice to the residents of their states.

- States legislatures respond more quickly than Congress to the needs of their constituents. The identity theft protections that do exist for consumers were pioneered in state legislatures.

- ID thieves are smart and adapt fast. Eliminating the ability of state legislatures to develop new anti-ID theft tools would give the crooks a longer head start on the consumer.

- States should be able to require that an entity which has a security breach take other steps even if Congress does not include all of those steps in a federal notice of

[1] After the loss of a back up tape containing unencrypted social security numbers, CitiFinancial still claimed that consumers were not a risk of harm. After 40 million card numbers were accessed by crooks using specially inserted computer code at a processor, MasterCard still claimed that consumers were not at risk of harm.

breach law, such as paying for a security freeze, paying for credit monitoring, providing live telephone customer assistance, or imposing fines if a required notice is not given. Congress shouldn't take these choices away from the states.

- Any concern about both a state and federal law requiring notice could easily be addressed by a provision in any new federal law that giving the stronger of the state or federal notice satisfies the requirement to give notice under both laws.

Bankers argue that they should not be covered by state or federal notice of breach laws because the federal banking regulators have issued "guidelines" on when banks and other financial institutions should notify consumers of security breaches.

Here is what the bankers aren't saying:

- The federal regulatory guidelines allow the bank (or other financial institution) to decide whether to notify you of a security breach.

- The bank has to notify you *only* if the information has already been misused or *the bank* determines that it is reasonably possible that the breached information will be misused.

- If the bank doesn't know who breached the system or stole the laptop or the back-up tape, how can it determine that you are at risk? A bank might argue that as long as it doesn't know who got into the system, it doesn't have to tell consumers about the intrusion.

- The regulators' explanation to the banks says that they don't even have to perform a full investigation before deciding that the consumer is not at risk.

- The regulatory guidance doesn't even cover non-consumers, such as small businesses whose data is compromised.

- The regulatory guidance doesn't cover all consumers, only those who are customers of the bank.

- The banking agencies claim that only they can enforce the regulatory guidance.

Prepared by:
Gail Hillebrand
Consumers Union of U.S., Inc.
415 431-6747
Additional contact:
Susanna Montezemolo
Consumers Union of U.S., Inc.
202 462-6262