2016 ABA Issue Summary

Cybersecurity

Contact: Sarah Grano, ABA Public Relations (202) 663-5470 or sgrano@aba.com

The financial services industry is the gold standard of cybersecurity.

- Banks and other financial services companies have made cybersecurity a top priority.
- Banks have the highest level of security among critical U.S. industries such as banking, energy and telecommunications and the most stringent regulatory requirements.
- It is important to build a cybersecurity environment that does not conflict with existing regulatory requirements or become a compliance exercise.

Protecting your money is a partnership.

- The bank and the customer have to work together to prevent fraud.
- Banks use a combination of safeguards to protect your information, such as employee training, strict privacy policies, rigorous security standards and encryption systems.
- Customers should monitor their accounts regularly and alert the bank right away if they suspect they are a victim of fraud.

Consumers are protected against losses.

- When a customer reports an unauthorized transaction, the bank will cover the loss and take measures to protect your account.
- The banking industry is committed to continuing its tradition of safeguarding confidential financial information.

Financial institutions already have a regulatory system in place.

- Unlike other businesses that have experienced security breaches, banks already have a regulatory system in place advising them how to respond and notify their customers.
- Federal regulators have issued guidance telling banks what to do if they have a security breach, including when to notify customers.
    - The guidance requires banks to immediately investigate breach incidents and determine if any fraud has occurred, even if it is "reasonably possible." If so, customers must be notified as soon as possible, unless law enforcement tells the bank that an investigation would be endangered by the notice.
    - If misuse of the data is unlikely, no notice is required, primarily to minimize customer inconvenience or cause undue alarm. Unnecessary warnings could run the risk of creating a "cry wolf" attitude to future notices.
    - Regardless of the likelihood of misuse, bank regulators must *always* be notified when illegal access occurs so that they can monitor the situation.

Cybersecurity

(continued)

Background:
All banks must develop and have in place a data breach-response program that contains the following five elements:

- The program can be risk-based – that is, based on the risk that a consumer might be harmed by the compromise of the information in the custody of that institution. This gives institutions some flexibility to decide if a notification is necessary;

- The institution must have a response and investigation system in place that can assess the situation;

- If sensitive information is involved, the institution's federal regulator must be notified;

- The institution must be able to take appropriate steps to contain and control the incident, including preserving records and other evidence; and

- Customers must be notified if they are reasonably deemed to be at risk, but in some circumstances there could be a delay in notification, especially where law enforcement tells the institution in writing that an investigation would be endangered by that notice.