

that would allow someone to log onto or access another person's account, such as user name and password.

Under the Security Guidelines, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. The Agencies believe that substantial harm or inconvenience is most likely to result from the improper access to and use of *sensitive customer information*. Accordingly, the proposed Guidance requires notice to mitigate or prevent substantial harm or inconvenience to a customer.

The Agencies note that the response program required under the proposed Guidance must address incidents involving the unauthorized access to or use of any form of customer information. However, the customer notice requirement applies only to security breaches involving *sensitive customer information*.

The proposed Guidance provides several examples the Agencies believe typify situations in which customer notification is required and those when it is not. As in other circumstances, the Agencies also expect financial institutions to notify customers upon the direction of the institution's primary Federal regulator.

The proposed Guidance discusses the content and delivery of customer notices. The notice should include a general description of the incident, and provide information to assist customers in mitigating potential harm, including a customer service number, steps customers can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

In addition, institutions are expected to inform each customer about the availability of the Federal Trade Commission's ("FTC") online guidance regarding measures to protect against identity theft and to encourage the customer to report any suspected incidents of identity theft to the FTC. Further, institutions should provide the FTC's Web site address and telephone number for purposes of obtaining the guidance and reporting suspected incidents of identity theft. Currently, the Web site address is <http://www.ftc.gov/idtheft>, and the toll free number for the identity theft hotline is 1-877-IDTHEFT.

The proposed Guidance also describes other forms of assistance that financial institutions have offered to their customers in incidents of this type. Financial institutions may wish to offer

such forms of assistance to their customers and describe them in the customer notice.

II. Request for Comments

The Agencies invite comment on all aspects of the proposed Guidance, including each component of the response program described in Paragraph II of the proposed Guidance. Please consider the following questions in formulating your comments:

- Should any component of the response program be clarified in some way and, if so, how?
- Are there additional components that should be included in a response program to address incidents involving unauthorized access to or use of customer information? If so, please describe the component, and the reasons that support it.

- Should each component of the response program be retained? If not, which components should be deleted and why?
- In preparing the proposed

Guidance, the Agencies have attempted to identify a standard that will lead to customer notice when appropriate. The Agencies recognize that there is a spectrum of alternatives for developing a requirement to notify customers. On one side of the spectrum is a standard that would require a financial institution to notify its customers every time the mere possibility of misuse of customer information arises. On the other side is a standard that would require an institution to notify its customers only when it becomes aware of an incident involving unauthorized access to customer information and, based on unusual activity in customers' accounts or other indicia of identity theft, knows that the information is being misused. The Agencies propose a standard that lies in the middle of this spectrum. The Agencies believe that no useful purpose would be served if notices were sent due to the mere possibility of misuse of some customer information because, in general, the notices should alert customers to those situations where enhanced vigilance is necessary to protect against fraud or identity theft. Rather, the Agencies believe that notice to customers should be required in a narrower range of instances involving the unauthorized access to *sensitive customer information*. The standard proposed here would require a financial institution to send notice to each affected customer when the institution becomes aware of an incident of unauthorized access to *sensitive customer information*, unless the institution, after an appropriate

investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers' accounts for unusual or suspicious activity. The Agencies invite comment on whether this is the appropriate standard for requiring customer notice. For commenters who believe that this standard is inappropriate, the Agencies request that these commenters state specifically their reasoning and offer alternative thresholds for requiring customer notice.

- The proposed Guidance defines *sensitive customer information* as a social security number, a personal identification number (PIN), password, or an account number in conjunction with a personal identifier. *Sensitive customer information* would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such as user name and password. The Agencies request comment on which, if any, additional types of information should be included in this definition, such as mother's maiden name or driver's license number.

- The Agencies invite comment on the potential burden associated with the customer notice provisions. For example, what is the anticipated burden that may arise from the questions posed by those customers who receive the notices? Should the Agencies consider how the burden may vary depending upon the size and complexity of the institution?

- As part of the response program, the Agencies describe certain corrective measures that an institution should take once an incident of unauthorized access occurs. One such measure is to "secure accounts." Is the discussion of securing accounts sufficiently clear to enable institutions to know what is expected of them when instances of unauthorized access occur? To what extent would contracts between financial institutions and service providers need to be modified, if at all, to comply with the proposed Guidance? How much burden, if any, will the Guidance impose on service providers?

- The Agencies also invite comment on whether the proposed standard should be modified to apply to other extraordinary circumstances that compel an institution to conclude that unauthorized access to information, other than *sensitive customer information*, likely will result in substantial harm or inconvenience to the affected customers.