



17

Cheryl A. Voigt  
Chief Compliance Officer  
KeyCorp  
127 Public Square  
Cleveland, OH 44114  
Tel: 216 689-5950

**Via Electronic Delivery**

October 14, 2003

Public Information Room  
Office of the Comptroller of the Currency  
250 E Street, SW, Mailstop 1-5  
Washington, D.C. 20219  
Attention: Docket No. 03-18  
Email: [regs.comments@occ.treas.gov](mailto:regs.comments@occ.treas.gov)

Chief Counsel's Office  
Office of Thrift Supervision  
1700 G Street, NW  
Washington, D.C. 20552  
Attention Docket No. 03-35  
Email: [regs.comments@ots.treas.gov](mailto:regs.comments@ots.treas.gov)

Ms. Jennifer J. Johnson, Secretary  
Board of Governors of the Federal  
Reserve System  
20<sup>th</sup> Street and Constitution Ave. NW  
Washington, D.C. 20551  
Attention: Docket No. OP-1155  
Email: [regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov)

Robert E. Feldman  
Executive Secretary  
Federal Deposit Insurance Company  
550 17<sup>th</sup> Street NW  
Washington, D.C. 20429  
Attention: Comments/OES  
Email: [comments@fdic.gov](mailto:comments@fdic.gov)

Re: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("the proposed Guidance")

Ladies and Gentlemen:

KeyCorp, a financial services company with assets of approximately \$83 billion, ("Key") appreciates the opportunity to comment on the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("the proposed Guidance") applicable to financial institutions. The security of customer information is always of highest priority at Key.

KeyCorp is committed to the protection of our customer's sensitive information. We have responded in the recent past with substantial efforts to protect this singularly most important asset of our business. Our safeguarding measures include a combination of encryption systems, rigorous standards, strict privacy policies, and employee training and awareness. In addition, implementation of the Customer Identification Program mandated in the USA Patriot Act

enhances new customer verification techniques that will have additional deterrence effects on identity theft crimes.

The proposed Guidance acknowledges the need for continued vigilance in the area of potential identity theft. The banking industry is acutely aware and responsive at the individual institution level to potential consequences that directly impact them through financial losses, various risk exposures, and loss of customer and shareholder confidence. KeyCorp is deeply concerned that the specific approach in the proposed guidelines will not allow for individualized assessment of different situations from business risk perspectives specific to each institution. As a responsible financial entity, we have put much attention into responding to the Security Guidelines established under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) and believe that these Security Guidelines provide sufficient guidance and direction for the protection of sensitive customer information. KeyCorp already takes significant measures to maintain excellent business relationships with our customers including respect for their privacy and security concerns.

### Conclusion

KeyCorp and the majority of financial institutions in the country over the past few years have paid significant attention to identity theft issues. Improved system access restrictions, refined processes to limit information use, improved encryption of data, increased employee training and awareness, and the development of policies and procedures surrounding the existing Security Guidelines have appropriately addressed business responses and risk assessments for incidents of unauthorized access of sensitive customer information. KeyCorp concludes Section 501(b) of the GLBA offers sufficient guidance pertaining to unauthorized access to sensitive customer information as it stands and needs no further Agency interpretation, clarification or modification. If Guidance is still considered necessary after further review and analysis, any proposed and final Interagency Guidelines must reflect the vast business experiences and practical operational issues and responses of the financial services industry. The Agencies should consider empanelling an Advisory Board comprised of institutions that would be substantially affected by these significant changes, which would then offer seasoned analysis, review and recommendations. At a minimum, another comment period should be provided to ensure the serious issues brought forth by the commenting institutions and organizations are appropriately addressed in any final Guidance.

### Observations

The proposed Guidelines are constrictive and do not permit a flexible risk based approach, as defined by the affected financial institution, to each individual incident.

All response programs to the unauthorized access to or use of sensitive customer information have elements of assessment, containment, and addressing harm to customers. The manner and method of this process is currently heavily dependent on the institution's size, operational and system structures, and risk tolerances and should remain as such. The Guidelines suggestions (which would quickly become "best practices", "minimum standards", then "mandates") include

“shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying access controls,” in situations that “could result” in substantial harm or inconvenience to the customer. These extreme measures are advanced to address incidents of potential, unpredictable criminal behavior if a customer is inconvenienced. The response determined by the financial institution should not be prescribed in such prohibitive, concrete terms while the individual nuances of each situation are not given due consideration.

Constraints are also visible in the Guidelines by the inclusion of notice to the institution’s primary regulator about any potential incident that remotely hints at unauthorized access to sensitive customer information. This threshold of regulatory notice for these incidents is unusually low and extremely burdensome for both regulatory agencies as well as the financial institution. While KeyCorp agrees that regulators should be informed of any significant incidents, the Guideline requirement for regulatory notice can be reasonably interpreted as encompassing all incidents.

Incidents involving encrypted sensitive customer data should be categorically and clearly exempted from any notice requirements.

Encrypted data, including relevant pieces of sensitive customer information, should be exempted from the notice requirements, both regulatory and customer. This exemption should also be applied if at least one piece of the required pieces of information is encrypted, as the remaining unencrypted information does not qualify as sensitive information. The storage and transmission of encrypted data is an accepted business practice that is widely acknowledged as a secure means of maintaining confidential information and the proposed Guidance should reflect that position.

Customer notice requirements, if required by regulation, should only be applicable to incidents and sensitive customer information under the control of the financial institution that are deemed to pose significant risk of substantial harm to a significant number of customers.

The proposed customer notice requirement is too expansive and includes “groups” of customers that may or may not be affected. The notice requirement, if one is established, should adhere to a much higher standard of scrutiny than *likely to occur* to a single individual after the financial institution takes appropriate steps. This simple characterization will certainly include customers who have no need to be concerned or anxious about theft of their identities. A notification requirement that errs on the conservative side will initially increase the customer’s anxiety and eventually, their apathy to these incidents. This is a serious risk of the notice requirement as proposed. Moreover, the value of the notice is questionable when the reality is in most situations a financial institution cannot possibly conclude, even after a thorough assessment of the situation, the potential for criminal behavior that may result in a particular customer’s potential financial loss or theft of identity. What concrete assistance a notice can provide is empathy and awareness for the future, however this benefit will be more than offset by the stress and anxiety the notice will surely create. Information as to what steps individuals can take to minimize the impact of identity theft, as proposed by the Guidelines, is more appropriately given in a proactive fashion by educating our customers and increasing their awareness before sensitive information has been breached.

The costs associated with widespread notice, both tangible and intangible, are potentially extreme. The concentration of necessary human resources at the financial institution to effectively support the type of notice process proposed (e.g. staffing and training a customer service area to answer calls) would be excessively costly and would eventually dramatically increase the cost of basic services to customers.

A less prescriptive model of customer notice would alleviate some of the heavy financial and reputation burden to the financial institution. Suggestions include providing a flexible time period for response and notice based on an assessment of the situation, deleting the superfluous requirements to “assist” the customer in updating consumer reports (which potentially could be a customer privacy violation, in and of itself) and the “offer to subscribe” the customer to a reporting service. All of these elements, as suggestions to be included in the notice, are cost prohibitive, restrictive and unlikely to be utilized as offers to the customers.

KeyCorp appreciates the opportunity to be an important part of the comment process surrounding appropriate response and notice to unauthorized access to sensitive customer information. The comments included here address the portions of the proposed Guidance that present the serious concerns from our perspective. We will continue to remain a collaborative partner with the Agencies, as this important topic is one of our highest business priorities. Thank you for your interest.

Sincerely,

Cheryl A. Voigt  
Chief Compliance Officer  
KeyCorp