



13

October 14, 2003

Public Information Room
Office of the Comptroller of the Currency
250 E Street, SW
Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 03-18

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal
Reserve System
20th Street and Constitution
Avenue, NW
Washington, DC 20551
Attn: Docket No. OP-1155

Robert E. Feldman
Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 03-05

Re: Proposed Interagency Guidance on Response Programs for Unauthorized
Access to Customer Information and Customer Notice

Ladies and Gentlemen:

This comment letter is submitted on behalf of MBNA America Bank N.A. ("MBNA") in response to the Notice and Request for Comment issued by the Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency, and Office of Thrift Supervision (collectively, "the Agencies") regarding the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" ("Proposed Guidance"). MBNA appreciates the opportunity to comment on this important issue.

MBNA supports the Proposed Guidance's conclusion that an aggressive response program is a key part of a bank's information security plan, and also supports the Agency's efforts to explore measures aimed at enhancing the security of customer information and reducing the deleterious effects of identity theft. However, key aspects of the Proposed Guidance do not effectively recognize the day-to-day realities of customer information security and suggest an overly rigid approach that is likely to be

both inefficient and harmful. In particular, a more balanced and flexible approach is needed to allow banks to develop and implement effective and efficient fraud prevention measures consistent with their overall security procedures, risk based strategies and business operations.

Notifying Regulatory and Law Enforcement Agencies

The Proposed Guidance states that “the institution should promptly notify its primary Federal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers.”¹ It also states that “substantial harm or inconvenience is most likely to result from improper access to sensitive customer information because this type of information is easily misused, as in the commission of identity theft.”² While MBNA agrees that the primary federal regulator should be promptly notified of a security breach involving customer information, it should only be required under certain circumstances. The compromise of customer information that is not sensitive customer information (“SCI”), as defined by the Proposed Guidance, is not likely to cause substantial harm or inconvenience since it is generally available through public documents. Even the loss of a single element of SCI, such as a personal identification number, without any other customer information, is not likely to cause substantial harm or inconvenience. The Proposed Guidance, as written, would require the bank or its service provider to make notification regardless of whether or not the unauthorized access is likely to result in substantial harm or inconvenience to the customer. This could cause regulatory and law enforcement agencies to be so inundated with reports that it would become impossible to separate actual from potential fraudulent activity. It would also require unnecessary monitoring on the part of the bank, and would be a drain on the limited resources of the regulatory and law enforcement agencies.

The final guidance should allow the banks the flexibility to determine, based on its own risk-based strategies, when to notify the primary regulator. The requirement to notify the customer is based on the principle that only a loss of SCI would be required to trigger notification, and then only if, after an appropriate investigation, the bank reasonably concludes that misuse of the information would cause substantial harm or inconvenience to the customer. MBNA agrees with the standard for providing notification to the customer and recommends that the same standard be applied to the requirement for notification of its primary federal regulator.

The Proposed Guidance also states that the “appropriate law enforcement authorities” should be notified by telephone. In many cases it is unclear what telephone number should be used. Since the size and sophistication of law enforcement authorities may differ from state to state the requirement to contact them by telephone may create confusion and unwarranted action by the law enforcement authority.

¹ 68 FR 47959 (August 12, 2003)

² 68 FR 47955, 47960 (August 12, 2003)

MBNA recommends that the final guidance provide that the filing of a SAR is sufficient notification.

MBNA further recommends that an exception be added that would suspend the customer notification requirement if law enforcement authorities notify the bank that such notification would impede an ongoing investigation, and would provide the bank with a safe harbor under these circumstances.

Flagging Accounts

The Proposed Guidance states that “the institution should immediately begin identifying and monitoring the accounts of those customers whose information may have been accessed or misused.”³ Banks typically have the capability to monitor for unusual activity, e.g., by monitoring for activity at merchants that the customer may have never used before, such as for gasoline purchases or convenience items, or for high-priced items such as jewelry or electronic equipment. They may also monitor for activity that is outside the customer’s typical geographical buying area. MBNA recommends that the final guidance should require a bank to flag only those accounts that the bank believes, based on its assessment of the situation and circumstances, are likely to have been compromised.

It is recommended that the Proposed Guidance give the bank the flexibility to monitor accounts for unusual activity. Short of closing every account where customer information has been allegedly compromised, it may be impossible to prevent unauthorized transactions on all such accounts. Accordingly, the final guidance should require the bank to use detective and preventive strategies where available and to provide personnel with information on how to handle fraudulent or suspicious activity, such as closing the account and making adjustments for fraudulent transactions. Although the Proposed Guidance does not specify how long an account should be monitored, other than to state (section II, paragraph D.3.b.) that the notice should remind customers of the need to remain vigilant, over the next twelve to twenty-four months,⁴ the final guidance should give the bank the discretion to determine when an account no longer warrants monitoring, based on its risk-based fraud and monitoring strategies.

Securing Accounts

The Proposed Guidance advises that when certain customer information has been accessed or misused the account should be “secured”. The Proposal provides no guidance on what is meant by “secure”. If securing the account means to stop all transactions, this could seriously inconvenience customers, particularly if the account receives automatic deposits or is used to make automatic payments for services or for other customer obligations such as mortgages or car payments. This will be particularly harmful if the account is secured only because there was an indication that the customer’s

³ FR 68 47955, 47959 (August 12, 2003)

⁴ *Id.*

information was purportedly accessed, but there is no indication that the account was misused or that there was an intent to use the information for illicit purposes.

The final guidance should define “securing an account” in a manner that allows the bank the flexibility to determine the best means to safeguard the account and protect its customer from harm based on its own risk-based strategy for determining the probability and severity of fraudulent use of account information. Indiscriminate securing or closing of an account until the bank and its customer agree on a course of action would create an unnecessary burden on, and inconvenience to, the customer, and generate unnecessary costs associated with customer inquiries and account replacement. In most cases customers are protected from fraudulent activity through federal regulations⁵, state laws, and bank and card issuer policies insulating the customer from liability for such activity.

Customer Notice and Assistance

The Proposed Guidance states that, “an institution should notify affected customers whenever it becomes aware 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”.⁶ This language could be confusing, as a bank might be inclined to inform its customers prior to obtaining the findings of its investigation. Premature notification could result in the customer needlessly closing their account out of fear of being compromised when that may not be the case.

MBNA recommends that the requirement for customer notification be reworded to provide that customer notification should be given if, after an investigation, the bank concludes that compromise of the information may result in substantial harm or inconvenience to the customer. Also, if the bank reasonably believes that the customer is a perpetrator of the fraudulent activity, notification to that customer should obviously not be required.

It is also recommended that, given the confusion and controversy over the readability of the Privacy Notice required by Regulation P, a sample notification be provided as an appendix to the final guidance.

Examples of When Notice Should Be Given

The Proposed Guidance uses an example that “when an employee of the institution has obtained unauthorized access to sensitive customer information maintained in either paper or electronic form customer notification should be sent.”⁷ In many cases employees of banks gain access to SCI inadvertently. This does not necessarily mean

⁵ 12 CFR 205, Electronic Funds Transfer (Regulation E) and 12 CFR 226, Truth in Lending (Regulation Z).

⁶ 68 Federal Register 47960 (August 12, 2003)

⁷ *Id.*

that the employee intends to use this information for illicit purposes. Although the preamble to this example states that notification should be sent unless after an appropriate investigation the bank can reasonably conclude that misuse of the information is unlikely to occur, this particular example by itself could cause confusion. MBNA recommends that this example be changed to state that if an employee has obtained unauthorized access to SCI maintained in either paper or electronic form, and the bank concludes that the employee intends to use or has used the information for illicit purposes, customer notification should be given.

In conclusion, MBNA appreciates the opportunity to submit comments on this very important matter. If you have any questions concerning these comments or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact Joseph R. Crouse at (302) 432-0716.

Respectfully submitted:
MBNA America Bank, N.A.
By /s/ Joseph R. Crouse
Joseph R. Crouse
Legislative Counsel