

22

**Comments Submitted by:  
Privacy Rights Clearinghouse  
Consumers Union of U.S., Inc.  
Consumer Action  
Privacy Activism**

October 14, 2003

Office of the Comptroller of Currency  
Public Information Room  
250 E. Street, Mail stop 1-5  
Washington, DC 20219  
**Attention Docket No 03-18**  
[regs.comments@occ.treas.gov](mailto:regs.comments@occ.treas.gov)

Bd. of Governors of Federal Reserve  
Jennifer J. Johnson, Secretary  
20<sup>th</sup> St and Constitution Ave, SW  
Washington, DC 20551  
**Docket No. OP-1155**  
[regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov)

Federal Deposit Insurance Corp  
Robert E. Feldman, Secretary  
550 17<sup>th</sup> St, NW  
Washington, DC 20429  
[comments@fdic.gov](mailto:comments@fdic.gov)

Office of Thrift Supervision  
Chief Counsel's Office, OTS (No. 3-35)  
1700 G Street, NW 20552  
Washington, DC 20552  
[regs.comments@ots.treas.gov](mailto:regs.comments@ots.treas.gov)

**RE: Interagency Guidance on Response Programs for Unauthorized Access to  
Customer Information and Customer Notice (Response Guidelines)**

The Privacy Rights Clearinghouse, Consumers Union, Consumer Action and Privacy Activism submit these comments on the proposed Response Guidelines published jointly by the Office of Comptroller of Currency (OCC), Board of Governors of the Federal Reserve (Board), Office of Thrift Supervision (OTS) and the Federal Deposit Insurance Corporation (FDIC), referred to as Agencies in this document.<sup>1</sup> The proposed guidelines supplement the Security Guidelines<sup>2</sup> adopted by the Agencies to fulfill the requirement of § 501(b) of the Gramm-Leach-Bliley Act (GLB).

The **Privacy Rights Clearinghouse** is a nonprofit consumer education and advocacy organization based in San Diego, CA, and established in 1992. The PRC advises consumers on a variety of informational privacy issues, including financial privacy and identity theft, through a series of fact sheets as well as individual counseling available via telephone and e-mail. It represents consumers' interests in legislative and regulatory proceedings on the state and federal levels. [www.privacyrights.org](http://www.privacyrights.org)

<sup>1</sup> 68 FR 155, August 12, 2003

<sup>2</sup> Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Security Guidelines), published at 12 CFR Part 30, App B (OCC); 12 CFR Part 208, App. D-2, and Part 225, App. F (Board); 12 CFR Part 364, App. B. (FDIC); and 12 CFR Part 570, App. B (OTS).

**Consumers Union** is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education, and counsel about goods, services, health and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union has actively supported a wide variety of state consumer protection laws, including in the areas of credit, finance, and disclosure, including identity theft prevention laws and anti-predatory lending laws. [www.consumer.org](http://www.consumer.org)

**Consumer Action** is a statewide non-profit consumer education and advocacy organization serving California consumers since 1971. It provides consumers with information and education on matters of telecommunications, privacy, predatory lending and banking/credit issues. Consumer Action advocates at the state and federal legislative levels for consumer rights in the policy areas of banking and credit, product safety, privacy and identity theft and other issues affecting the quality of life of California consumers. [www.consumer-action.org](http://www.consumer-action.org)

**PrivacyActivism** San Francisco-based nonprofit consumer advocacy organization whose overall mission is to enable people to make well-informed decisions both on a personal and societal level about the importance of privacy. It examines the privacy risks associated with data collection. [www.privacyactivism.org](http://www.privacyactivism.org)

The Agencies' current proposal establishes guidance for financial institutions' response programs for unauthorized access to customer information. The proposal also includes guidance on when notice to customers is necessary.

Recent studies have confirmed that the crime of identity theft claims millions of victims each year, costing both victims and financial institutions billions of dollars in losses.<sup>3</sup> Financial institutions that collect and maintain personal customer information as part of business operations have a legal obligation to establish security procedures to maintain the confidentiality and integrity of that data.

A necessary component of any security procedure is a plan of response in the event that personal data is at risk of being compromised. For consumers, notice of even a potential breach is necessary to prevent or quickly remedy the problem if a financial institution's information security systems fail.

The Agencies' guidelines for response plans set the minimum necessary to avoid violations of the Security Guidelines. The following comments are provided as key consumer protection safeguards that should be included in the minimally acceptable response plan.

---

<sup>3</sup> "How Many Identity Theft Victims Are There? What Is the Impact on Victims? Recent Surveys and Studies from the Identity Theft Resource Center, Federal Trade Commission, Gartner, and Privacy & American Business" <http://privacyrights.org/ar/idthefts-surveys.htm>. The September 2003 survey by the Federal Trade Commission found there were nearly 10 million victims of identity theft in 2002. <http://www.ftc.gov/opa/2003/09/idtheft.htm>

**1. Definition of sensitive customer information.** The proposed guidelines define “sensitive customer information” as a “Social Security number, a personal identification number (PIN), password, or an account number in conjunction with a personal identifier.” This definition should be expanded to include other items of personal information commonly used to access accounts, including (1) mother’s maiden name (2) driver’s license number and (3) date of birth.

In addition, the definition of “sensitive customer information” should be revised to make it clear that a compromised account number, with or without an associated PIN, warrants resort to the response plan. There are many ways to access an account number, not all of which involve use of a PIN. The theft of an account number alone might not allow a thief to access an account through online banking. However, an account number alone is sufficient to create fraudulent checks. Moreover, some merchants have announced the use of automated clearinghouse debits online, which can be created with only a checking account number.

**2. Form of information.** It should be clear that the guidelines apply to information maintained and stored in all forms, including paper as well as computerized format. The guidelines should also make clear that response procedures should be developed for any unauthorized means of access. Unauthorized access and misuse of personal data is all too often seen as the result of computer intrusions. However, it is not uncommon for unauthorized access to be the result of theft or inadequate destruction of paper records.

For this reason, the guidance must specify that it encompasses (1) *all records containing sensitive customer information* that is accessed by (2) *any unauthorized means*. This clarification may be accomplished by incorporating the definitions of “*customer information*” and “*customer information systems*” from the Security Guidelines.

**3. Scope of unauthorized access.** The tone of the proposed guidelines as well as the listed examples of when notice should be given to consumers suggest that the guidelines are limited to instances of widespread breaches of security involving numerous customers. Without explicit guidance to the contrary, financial institutions may be free to develop response plans that are only triggered when a certain number of customer accounts are involved. Thus, the consumer whose information is, for whatever reason, disclosed in an unauthorized manner could be denied the benefit of notice necessary to take preventive measures.

The consumer whose information is disclosed in an isolated incident is at no less risk than the consumer whose information is disclosed along with hundreds or thousands of others. The PRC has been contacted many times by consumers whose loan applications or other personal information has been inadvertently mailed to another consumer. In such cases, consumers are advised to contact management at the financial institution involved as well as report the breach to the appropriate regulator. The guidelines should explicitly require that the response plan be put into effect and customer notice provided regardless of the number of consumers affected by an unauthorized disclosure.

**4. Notice to regulators** is a required part of a financial institution’s response plan. However, it is unclear from the proposed guidelines whether notice to regulators is required for all security breach incidents or only those instances the Agencies have identified as warranting notice to

affected consumers. The guidelines require notice to customers when sensitive customer information has been improperly accessed, *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.*

The ability to conduct its own investigation and reach conclusions about the likelihood of misuse of customer data gives institutions wide latitude in determining a course of action. While not all instances of improper access necessarily require notice to customers, any event that triggers an internal investigation by the institution should require notice to the appropriate regulator. In this way, regulators will be able to assess the effectiveness of response plans, and, where appropriate, direct notice to customers.

Such a procedure establishes an early warning for regulators and creates a needed safeguard for personal data by giving the oversight agency, and not the institution, ultimate authority to assess the *need to disclose*. With agency review, the risk of bad publicity is less likely to weigh too heavily in deciding when notice is necessary.

**5. Institution's obligations to customer.** As the Agencies note, financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. In the event of an unauthorized access, the institution's obligations to the customer must be clearly explained by the Agencies in adopting final Response Guidelines.

First, the guidance should impose an explicit obligation on the part of institutions to cooperate with customers whose information has been the target of an unauthorized access or use. This should include the obligation to provide customers whose identity has been compromised with all documents related to the theft, including application and transaction information on the account opened or attempted to be opened by the identity thief. This duty should include a timeline, such as the 10 business days after request provided for in California Penal Code section 530.8.

Second, the guideline should create an obligation on the part of institutions to correct erroneous information on the consumer's credit report that results from the unauthorized access. This obligation to cooperate and correct erroneous information should extend to all other consumer reports as well. Negative information on a credit report may impact the consumer's life far beyond the ability to get credit. Bad credit marks can affect a consumer's employment, insurance premiums, and ability to rent an apartment. It is important that negative information on all consumer reports be cleansed with the cooperation of the financial institution involved.

Consumers whose checking accounts are compromised by a security breach may, for example, have an unwarranted, erroneous entry on their ChexSystems Report. Such an entry, even though false, could prevent the consumer from opening an account at another financial institution.

The Agencies' guidance should be clear that the financial institution's obligation and duty to its customer extends to all accounts held by affiliates and subsidiaries of the financial institution. This is particularly important for insurance customers of the financial institution since a dominant factor in insurance underwriting and risk assessment is the consumer's credit history.

This duty to cooperate with consumers and correct erroneous information resulting from a financial institution's security breach can only be effective if the institution's response plan incorporates the spectrum of corporate affiliations.

6. **Application for new credit.** The proposed guidelines require financial institutions to flag and secure *existing* customer accounts following an incident. However, the guidelines should also require monitoring the use of *sensitive customer information* for new credit. Close scrutiny is particularly warranted where an application for new credit includes a change of address, new passwords, or any variance in *sensitive customer information* previously known to the financial institution or noted when the financial institution examines the individual's credit report. Extra precaution is necessary because only some instances of unauthorized access trigger notice to customers.

When a financial institution – or, as should be, the institution's primary regulator – decides an incident does not require notice to customers, the institution assumes greater responsibility to ensure data security. Instances that do not result in notice give the consumer no opportunity to independently prevent or mitigate harmful consequences.

Applications for new credit could indeed be an early warning that sensitive data has been compromised by an identity thief. Thus, financial institutions cannot limit monitoring to *existing* accounts but must be vigilant in monitoring *all uses* of *sensitive customer information*. The Federal Trade Commission's survey on identity theft, reported September 2003, found that there were nearly 10 million victims of this crime in 2002, with one third of them being cases of new account fraud, also known as application fraud.<sup>4</sup>

New account fraud is the most devastating form of financial identity theft for victims. Individuals are not likely to learn that someone has opened new accounts in their name until they themselves attempt to open new credit accounts, obtain a mortgage, refinance their home, or rent an apartment – at which time the creditor obtains a credit report and learns that the individual has a bad track record. The victim is then burdened with regaining his/her financial health and clearing the credit report of the fraudulent trade lines. This can take many months, even years. During that time the victim is in credit limbo. It is difficult to obtain reasonably-priced credit, rent an apartment, even in some cases to obtain employment.

We do not know if the Agencies meant to overlook new account fraud in their Response Guidelines. Certainly, notifying individuals who do not have existing accounts with the financial institution that an application appears to have been made fraudulently in their name is a vitally important aspect of identity theft prevention. This type of notice should not be overlooked in the Response Guidelines.

7. **Fraud alerts.** The guidelines should *require* financial institutions to observe fraud alerts in the customer's consumer reports. To be an effective deterrent against identity theft, a fraud alert must prompt a reasonable investigation by the financial institution before extending new credit or changing the terms of existing credit. The Privacy Rights Clearinghouse has assisted

---

<sup>4</sup> "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," (September 3, 2003) <http://www.ftc.gov/opa/2003/09/idtheft.htm>

thousands of identity theft victims in the past decade. A significant number of victims have reported to the PRC that a credit card company issued credit to the imposter *after* the victim placed fraud alerts on his/her credit report.

8. **Time for delivery of notice to customers.** The proposed guidelines state only that customer notice should be *timely*, thus giving financial institutions wide discretion about when notice should be given. This vague requirement of timeliness is unacceptable and an inadequate defense against identity theft. Criminals who obtain sensitive consumer data through any illegal means are more likely than not to begin using that information immediately to run up credit card charges, drain the consumer's account, or open new accounts.

The Agencies should define what it means by *timely* and set an absolute maximum on the time for notice to consumers. Considering the need to act expeditiously against identity theft, an outside limit of 48 hours (two business days) after the institution learns of the breach is a reasonable and timely requirement for notice to customers.

9. **Means of notice to customers.** The guidelines should explicitly state that general notice on a financial institution's web site is inadequate. The Agencies should make it clear that notice to customers under response plans requires individual notice, either by certified postal mail or an e-mail if the customer conducts business with the institution online.

The proposed guidelines say also that the notice to customers should include a phone number that customers can call for further information and assistance. The guidelines should be more specific about the telephone number required to be included with notice to consumers.

First, the number should be toll free. Second, the telephone number should not be the institution's regular consumer assistance number where consumers may become mired in a selection of recorded choices. Instead, for instances of unauthorized access to customer data, the institution should establish a dedicated line, with trained staff, for use only for a particular breach of security. That same line should be maintained specifically for the purpose of assisting customers for that particular incident of breach.

The proposed guidelines suggest customers be reminded to remain vigilant over the next 12-24 months. This is also an appropriate time for the institution to maintain a phone number dedicated to each incident of unauthorized access.

10. **Assistance to customers.** The guidelines for assistance to customers should require that financial institutions independently notify credit and other consumer reporting agencies of the security breach to the customer's account. This is not expected to be an added burden to financial institutions, since companies regularly report account status to consumer reporting agencies.

If the affected department of the financial institution does not independently report the breach, there is a likelihood that the department that *reports* account status will inadvertently report erroneous information. In addition, an independent contact by the institution only alerts the credit agency to the possibility of erroneous information. This benefits the consumer by reinforcing the

fraud alert and also provides the evidence necessary for the consumer reporting agency to conduct its obligatory investigation of disputed information.

11. **State laws.** The guidelines should be clear that financial institutions must also comply with additional state law obligations. For example, California law imposes a statutory duty to provide information to identity theft victims (Penal Code 530.8). In addition, California has other identity theft protection and prevention statutes generally applicable to all companies doing business in the state. One example is California's document destruction (shredding) law (Civil Code 1798.80-1798.84). The Response Guidelines should explicitly state that they create a baseline set of obligations, and that a state can hold a financial institution to higher standards or to consistent additional standards. Otherwise, financial institutions may argue that they are excused from basic state data security and identity theft prevention statutes that apply to all others doing business in a state.

12. **Service providers.** The Security Guidelines require financial institutions to incorporate security measures into contractual agreements with service providers. The proposed guidelines for response programs should require service providers to report incidents to financial institutions within a certain time, no more than 24 hours after discovery of the incident.

The Response Guidelines should also be clear that the obligations on service providers also include joint marketers. This is consistent with the Agencies' privacy regulations. 12 CFR 216.13(b), the Board's version of the privacy regulations, states:

*(b) Service may include joint marketing.* The services a nonaffiliated third party performs for you under paragraph (a) of this section may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between you and one or more financial institutions.

Without this clarification, vast amounts of sensitive customer data shared for joint marketing purposes may not be subject to the response plan guidelines.

13. **Subscription services, credit monitoring programs.** This optional element for the response plan gives financial institutions a choice of informing customers about subscription services or offering to subscribe the customer to such a service free of charge. Only the latter option is appropriate for the response plan.

A customer whose sensitive information is accessed due to a financial institution's security systems failure should not be solicited for credit monitoring services. If monitoring services are part of the response plan at all, it should be offered as free to the customer. Customers encouraged to subscribe may be misled into believing that the purchase of a monitoring service is required for data security. Providing the customer with specific names of monitoring services also promotes commercial alliances between the financial institution and the monitoring service. Then, the potential exists for the focus to be on marketing the monitoring service rather than security for customer data.

**In closing**, we wish to draw your attention to a new publication of the California Office of Privacy Protection, "Recommended Practices on Notification of Security Breach Involving Personal Information" It is available on their web site at <http://www.privacy.ca.gov/recommendations/secbreach.pdf>.

In 2002, the California Legislature passed a law<sup>5</sup> that requires companies to notify individuals when a security breach has resulted in information about customers and/or employees getting into the hands of someone who potentially could use that information to commit identity theft. The Office of Privacy Protection has published a set of recommended practices to guide organizations of all types – companies, government agencies, and nonprofits – in notifying individuals whose personal information has been compromised. You might find this guide instructive as you consider the best approaches to take in the Response Guidelines.

Thank you for your consideration of these comments. Feel free to contact the Privacy Rights Clearinghouse if you have questions regarding the comments. The PRC will coordinate your questions with the other participating organizations.

Sincerely,

Beth Givens, Director  
Tena Friery, Research Director  
Privacy Rights Clearinghouse  
San Diego, CA  
Telephone: (619) 298-3396  
Email: [bgivens@privacyrights.org](mailto:bgivens@privacyrights.org)  
[tfriery@privacyrights.org](mailto:tfriery@privacyrights.org)

Gail K. Hillebrand  
Senior Attorney  
Consumers Union West Coast Regional Office  
San Francisco, CA

Ken McEldowney  
Executive Director  
Consumer Action  
San Francisco, CA

Deborah Pierce  
Executive Director  
PrivacyActivism  
San Francisco, CA

---

<sup>5</sup> California Senate Bill 1386 and Assembly Bill 700, codified at California Civil Code Sections 1798.29 and 1798.82 - 1798.84. [www.leginfo.ca.gov](http://www.leginfo.ca.gov)