

# QUARTERLY REPORT

MISSISSIPPI REGULATORY COMPLIANCE GROUP

February 2008

Vol. 19 No. 1

## FEDERAL RESERVE PROPOSES NEW TRUTH-IN-LENDING/HOEPA RULES

Responding to widespread concern and discussion over the impact of practices in the so-called subprime lending market on the housing market and the U.S. economy, the Board of Governors of the Federal Reserve has proposed regulations to amend Regulation Z aimed at protecting consumers from “unfair, abusive, or deceptive lending and servicing practices.” Among other things, the proposed new regulations create a newly defined category of loans - “higher priced mortgage loans” - for which special rules will apply. Also, the regulations propose to place certain additional protections on all mortgage loans secured by a consumer’s principal dwelling, regardless of loan price; and place new requirements on advertising that are designed to provide, accurate and balanced information in a clear and conspicuous manner about rates, monthly payments, and other loan features. Finally, the proposal would require that consumers be provided with transaction-specific mortgage loan disclosures before paying any fee, except a reasonable fee for reviewing credit history.

Historically, the HOEPA regulations contained in Regulation Z have placed specific restrictions on high cost loans secured by a consumer’s principal dwelling, with high cost being defined by reference to the interest rate and/or fee structure of a mortgage loan. Over time it has become apparent that the “subprime” loan market captures an increasingly broad range of loan products, designed for borrowers who are perceived to have high credit risk. For example, the Federal Reserve cites estimates that in 2001, subprime loans represented about 9 percent of loan originations, and that amount doubled to 20 percent by 2005 and 2006. In addition, the Federal Reserve states that delinquencies in

excess of 90 days for subprime loans were about 13 percent in October, 2007, which is twice the rate for a similar period in 2005.

In presenting the proposed new regulations, the Federal Reserve states that the federal financial institution regulatory agencies have issued various forms of guidance to regulated financial institutions to promote safe and sound practices when making subprime loans, however this guidance only applies to a limited segment of lenders participating in the subprime market. Due to the size and scope that the subprime market has attained, and the fact that a large number of lenders other than regulated financial institutions participate in originating subprime loans, the Federal Reserve believes that a specific regulatory scheme must be adopted to address the practices that have created problems in the subprime market. The Federal Reserve believes that only through amendments to Regulation Z can all participants in the subprime market be held accountable to higher, more protective standards that hopefully will prevent further problems in the future.

Federal Reserve Proposes New Truth-in-Lending/HOEPA Rules .....	1
Regulatory Agencies Release “Red Flag” Guidelines as Final Rule .....	3
Fair Credit Reporting Affiliate Marketing Regulation .....	6
Federal Reserve Board Amends Regulations to Provide Disclosures in Electronic Form .....	11
Good News and Bad News Regarding BSA....	13
Interagency Statement on Pandemic Planning	13
MRCG February Meeting To Be Held on February 14, 2008 .....	15
MRCG Compliance Calendar .....	16

As mentioned previously, a cornerstone of the proposed Regulation Z amendments is the extension of new protections to a category of consumer residential mortgage loans defined as “higher-priced” mortgage loans. Under the proposals, a lender would be prohibited from engaging in certain specific practices or activities when making a “higher priced” mortgage loan, including:

- (1) engaging in a pattern or practice of making higher priced mortgage loans based on the collateral, without regard to repayment ability of the borrower;
- (2) making an individual a higher-priced mortgage loan without verifying consumer income and assets that will be relied upon for repayment;
- (3) imposing prepayment penalties except under certain conditions; and
- (4) structuring a closed-end mortgage as an open-end line of credit for the purpose of evading the restrictions on higher-priced mortgage loans, which would not apply to open-end lines of credit.

Additionally, a lender will be required to establish an escrow account for taxes and insurance in connection with any higher-priced, first-lien mortgage loan if the proposed amendments are adopted in final form.

The proposed definition of a “higher priced” mortgage loan relates solely to the interest rate on the loan. Specifically, a higher priced mortgage loan would be defined as either a first lien loan with an APR at least 3 percentage points in excess of the yield on US Treasury securities with a comparable term, or a second lien loan with an APR at least 5 percentage points in excess of such comparable US Treasury yield. The definition excludes home equity lines of credit, reverse mortgages, construction-only loans, and bridge loans. The regulation also would not apply to loans that are not secured by a consumer’s principal dwelling, such as loans on investment property.

The Federal Reserve acknowledges that the interest rate limits described in the definition of higher priced loans may be expansive enough to include some loans falling between the true subprime and prime markets. An important part of the comment process and further revision and refinement of the regulation will likely involve the defined parameters of higher priced mortgage loans.

While the proposed regulations briefly summarized above would be designed to apply to higher priced mortgage loans, other proposed regulations would apply to all mortgage loans secured by a consumer’s principal dwelling, regardless of pricing or other characteristics. These restrictions include:

- (1) A prohibition against paying a mortgage broker in connection with a covered mortgage loan transaction unless the payment does not exceed the amount the broker has agreed to in advance with the consumer as being the broker’s total compensation. The broker compensation must be disclosed as a dollar amount, not a range of fees or a percentage.
- (2) The broker and the consumer must enter a written agreement stating the fee permitted as described above in item (1), and the agreement must contain a disclosure that a creditor’s payment to a broker can influence the broker to offer the consumer loan terms or products that are not in the consumer’s interest or are not the most favorable the consumer could obtain.
- (3) The agreement between the consumer and the broker must be entered before the consumer pays a fee to any person in connection with the transaction or submits an application.

These proposed regulations related to mortgage brokers would not apply to employees of the lender. The Federal Reserve also contemplates coordinating the final regulations with changes that may be imposed by HUD in connection with RESPA regulations concerning disclosure of payments to mortgage brokers.

The Federal Reserve has also addressed perceived problems in mortgage loan servicing practices on mortgage loans generally through the proposed new regulations. New regulations would prohibit mortgage loan servicers from (a) failing to credit a consumer's periodic payment as of the date received, (b) imposing a late fee or delinquency charge on amounts owed on a previous late fee or delinquency charge, (c) failing to provide a current schedule of servicing fees and charges within a reasonable time of request, or (d) failing to provide an accurate payoff statement within a reasonable time of request. These regulations are proposed in response to evidence of possible excessive fees charged by mortgage servicing providers, especially in foreclosure situations. These proposed regulations would apply to both prime and subprime loans that are secured by a consumer's principal dwelling.

Advertising practices for open-end home equity plans and for closed-end credit that are secured by residential mortgages are also subject to new regulations in the Federal Reserve proposal. Both the open-end and closed-end provisions emphasize a clear and conspicuous standard for advertising disclosures. In the context of open-end credit, for example, the proposal clarifies that the clear and conspicuous standard applies to advertisements of plans that provide for introductory rates or payments. The clear and conspicuous standard for both open-end and closed-end credit would be consistent with the standards used in Regulation M concerning consumer leasing transactions. The regulations would require that closed-end credits describe the full range of rates and payments that may apply to a loan, without placing undue emphasis on "teaser" rates. The proposed advertising regulations will apply to print, internet, television, and oral advertisements. In addition to implementing the "clear and conspicuous" standard, the proposed regulations will specifically prohibit certain advertising practices deemed to be unfair and deceptive.

This article provides the most brief summary and overview of what are very lengthy, comprehensive, and complex proposed revisions to Regulation Z. These regulations, when finally

implemented, will have far reaching effect on lenders of all sizes, and indeed on the way that mortgage loans are originated. In the upcoming quarterly meetings, we will present and discuss some of the most significant and relevant aspects of these proposals for your review and input. We have been asked by the Steering Committees of both groups to prepare and submit a comment letter to the Federal Reserve expressing particular concerns that you have over these regulations and the impact they may have on your business and compliance practices. Please remember to compile your list of questions, concerns or matters for clarification on the proposed amendments to Regulation Z, so that we may compile as complete a comment letter as possible for submission to the Federal Reserve.

<Virginia Wilson>

## **REGULATORY AGENCIES RELEASE "RED FLAG" GUIDELINES AS FINAL RULE**

On November 15, 2007, the various bank regulatory agencies jointly released the final rules and guidelines on identity theft "red flags" and address discrepancies which implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.

This new final rule is divided into three parts:

- Duties of users regarding address discrepancy;
- Duties regarding the detection, prevention and mitigation of identity theft; and
- Duties of card issuers regarding changes of address.

Each of these topics is addressed below.

### **Duties Regarding Address Discrepancies.**

These duties arise whenever a user of a credit report receives notice from the credit bureau of a discrepancy between the consumer's address used to request the report and the consumer's

address contained in the credit bureau's own records.

A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report anytime the user receives a notice of address discrepancy.

The final rule provides examples of reasonable policies and procedures that a user could adopt. One example is comparing the information in the credit bureau report with information that the user obtained by following the requirements of its CIP policy. Another example would be comparing the information in the credit bureau report to the institution's own records such as applications, change of address notifications, or other customer account records.

Another possibility would be simply verifying the information in the credit bureau report directly with the consumer.

A further requirement of this portion of the final rule requires a user to develop and implement reasonable policies and procedures for furnishing an address for the consumer after the user has taken reasonable steps to confirm the accuracy of the address. However, the user incurs this obligation only if three conditions are met:

- The user can form a reasonable belief that the consumer report relates to the consumer that was inquired about;
- The institution establishes a continuing relationship with the consumer; and
- The institution regularly and in the ordinary course of business furnishes information to the consumer reporting agency.

The final rule provides examples of ways to confirm that an address is accurate. These examples include:

- Verifying the address with the consumer;
- Reviewing the institution's own records to verify the address of the consumer;

- Verifying the address through a third party; or
- Using other reasonable means.

The final rule requires a user that confirms a consumer's address where a discrepancy has been noted to furnish the consumer's correct address to the credit bureau during the regular reporting period in which the institution establishes a relationship with the consumer.

### **Duties Regarding the Detection, Prevention and Mitigation of Identity Theft.**

This portion of the Red Flag Guidelines is perhaps the most important part of the final rule. The final rule requires an institution to establish an Identity Theft Prevention Program, the details of which will be discussed at length below.

These requirements apply to all institutions that maintain "covered accounts." A "covered account" is defined a continuing relationship established by a person with an institution in order to obtain a product or service for personal, family, household or business purposes, including extensions of credit and deposit account relationships. It is important to note that the final rule specifically encompasses accounts for which there is a reasonably foreseeable risk to customers or the institution from identity theft, including financial, operational, compliance, reputation, or litigation risks. Products and services provided to business customers fall within the definition of a covered account.

Although it is readily apparent that banks offer covered accounts, the final rule requires all institutions to periodically determine whether they offer or maintain covered accounts. Institutions are instructed to conduct a risk assessment taking into consideration:

- The methods it provides to open accounts;
- The methods it provides to access accounts; and
- The institution's previous experiences with identity theft.

### **Establishment of an Identity Theft Prevention Program.**

An institution that offers covered accounts is required to develop and implement a written Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or the operation of an existing covered account. The Program should be appropriate to the size and complexity of the institution.

The final rule lists several elements of an Identity Theft Prevention Program. The first element is to identify relevant Red Flags for the particular institution and incorporate those Red Flags into the Program. The second element requires reasonable policies and procedures to detect Red Flags incorporated into the Program when they occur. The third element requires an appropriate response to any Red Flags detected in order to prevent and mitigate identity theft, and the fourth element requires the institution to ensure that the Program is updated periodically.

An institution must provide for continuing administration of the Program and must obtain approval of the initial written Program from its board of directors or an appropriate committee of the board. Proper ongoing administration of the Program requires involvement of the board of directors or a committee thereof or an appropriate senior management official in the ongoing administration of the Program. Staff must be trained to effectively implement the Program, and the institution is required to exercise appropriate and effective oversight of any service provider arrangements that could have identity theft implications.

Appendix J to the final rule provides guidelines for development of an institution's written identity theft Program. In designing its Program, an institution should incorporate its existing policies and procedures that could impact the foreseeable risks of customer identity theft, e.g., its CIP policy. In addition, an institution should consider the following facts:

- The types of covered accounts it offers;

- The methods it provides to open covered accounts;
- The methods it provides to access covered accounts; and
- The institution's previous experience with identity theft.

The final rule instructs institutions to consider several sources of relevant Red Flags, including the institution's own experience with identity theft, applicable supervisory guidance, and any other methods of identity theft it has identified.

To help an institution develop its Program, the final rule lists five categories of Red Flags to be considered:

- Alerts, notifications, or other warnings received from consumer reporting agencies;
- The presentation of suspicious documents by an applicant;
- The presentation of suspicious personal identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to, a covered account; and
- Notice from customers, victims of identity theft, law enforcement authorities, or others.

Supplement to Appendix J provides a number of examples of possible Red Flags that could be grouped under the aforesaid categories. In developing a Program, an institution should consult those supplementary examples.

The Program's policies and procedures should address the detection of Red Flags through the policies and procedures in place under an institution's Customer Identification Program Rules and authenticating a customer's identity, monitoring transactions, and verifying the validity of change of address requests for covered accounts.

The Program's policies and procedures should provide for appropriate responses to the Red Flags, taking into account possible aggravating factors such as a data security breach or notice of a fraudulent attempt to obtain a customer's

identifying information. Appropriate responses might include:

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, etc.;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account;
- Notifying law enforcement; or
- Determining that no response is warranted.

An institution's Program should be updated periodically based upon such factors as the experience of the institution with identity theft, changes in methods of identity theft, changes in methods to detect or mitigate identity theft, changes in the type of accounts offered, and changes to the institution's business, e.g., mergers, acquisitions, etc..

Oversight of the Program should be specifically assigned to either the board of directors, a committee of the board or a designated member of senior management.

#### **Duties of Card Issuers Regarding Changes of Address.**

This provision of the final rule applies to an issuer of a debit or credit card and requires the card issuer to establish and implement reasonable policies and procedures to assess the validity of a change of address request if it receives that request and within a short period of time thereafter (generally 30 days) it receives a request for an additional or replacement card. The final rule prohibits the issuer from issuing the card until, following its established procedures, the card issuer:

- Notifies the cardholder of the request either at the cardholder's former address or by some other means of communication that

the issuer and the cardholder have previously agreed to; and

- Provides to the cardholder a reasonable means of promptly reporting incorrect address changes.

A card issuer may otherwise assess the validity of a change of address by following the policies and procedures used to implement the institution's Identity Theft Prevention Program.

Institutions are free to comply with these new FACT Act requirements at the present, but compliance is mandatory by November 1, 2008. Obviously, considerable time and attention will be devoted to the implementation of the Identity Theft Prevention Program and the necessary policies and procedures to be adopted over the course of our next two quarterly meetings.

<Ed Wilmesherr>

### **FAIR CREDIT REPORTING AFFILIATE MARKETING REGULATION**

---

The last regulatory pieces of the FACT Act are finally falling into place. One of those is the Affiliate Marketing Regulations issued in November by the federal bank regulators. The new regulations implement Section 214 of the FACT Act which generally provides that a person may not use certain types of information about a consumer that is received from an affiliate for the purpose of making marketing solicitations to the consumer without first giving the consumer notice and an opportunity to opt out of the use of the information. Proposed regulations were issued in 2004. Final regulations became effective January 1, 2008 with a mandatory compliance date of October 1, 2008.

The affiliate marketing rules differ significantly from existing privacy and information sharing restrictions in that they govern the use of consumer report type information obtained from an affiliate rather than the sharing of the information. The regulations refer to the type of consumer information covered as "eligibility

information.” The meaning of that term needs to be understood in relation to existing Fair Credit Reporting Act (FCRA) provisions.

Under the FCRA, a person, such as a bank or other lender, may share information with third parties, affiliated or non-affiliated, about actual transactions or experiences (e.g., loan payment history) without becoming a consumer reporting agency. In addition, a person may share consumer report type information other than actual experience or transaction information (e.g., a credit score or information taken from a loan application) with its affiliates without becoming a consumer reporting agency if the consumer is first given notice and an opportunity to opt out before information is shared.

The new affiliate marketing regulations govern the use of information by an affiliate, not the sharing of information among affiliates, but the new rules apply to use of both transaction or experience type information as well as “other” consumer report type information. “Eligibility information” means any information bearing on a consumer’s credit worthiness, credit capacity, character, reputation, personal characteristics or mode of living, without regard to the exclusions from the FCRA definition of “consumer report” for transaction or experience information or information shared with an affiliate after notice and an opportunity to opt out has been given to the consumer. It is virtually all of the information about a consumer you derive from doing business with the consumer. In general, the regulations prohibit a bank or subsidiary from using eligibility information received from an affiliate about a consumer to make a marketing solicitation to the consumer unless: (i) clear and conspicuous notice in writing is given to the consumer that eligibility information about the consumer received from the affiliate may be used to make marketing solicitations to the consumer, (ii) the consumer is provided a reasonable opportunity and a reasonable and simple method to opt out and prohibit the use of the information for that purpose, and (iii) the consumer, in fact, has not opted out.

All of that sounds relatively straight forward, but the devil is in the details, as the saying goes. Fortunately, many examples are provided in the regulations to aid in their interpretation. Let’s start at the beginning with what constitutes making a solicitation.

A solicitation basically means the marketing of a product or service to a particular consumer based on eligibility information about the consumer received from an affiliate. A solicitation includes a telemarketing call, e-mail, direct mail or other form of marketing communication but excludes marketing communications aimed at the general public such as television, radio, billboard and newspaper advertisements. You “make” a solicitation covered by the rules if you receive eligibility information from an affiliate; you use that information to either: identify the consumer or type of consumer to receive a solicitation, establish criteria used to select the consumer to receive the solicitation, or tailor your solicitation or decide which of your products or services to market to the consumer; and as a result of your use of the information, a solicitation is provided to the consumer.

A critical factor in determining whether the rules apply is who actually uses eligibility information provided by an affiliate. The affiliate marketing rules do not prohibit receiving eligibility information from an affiliate or storing that information in a common database available to all affiliates (however, the information sharing rules under FCRA could). The new rules prohibit the use of that information for marketing purposes by someone other than the entity that collected it and that has the relationship with the consumer.

For example, assume a mortgage company affiliated with a bank wants to provide the bank with eligibility information obtained from mortgage loan applicants so the bank may market its home equity products to the consumers. Before the bank can use that information, notice and a reasonable opportunity to opt out must be given to each affected consumer. On the other hand, if the bank provides marketing materials to the mortgage

company along with the bank's own criteria for determining which home loan applicants it wants to market to, and the mortgage company then uses its own eligibility information to identify those consumers and makes the solicitations on behalf of the bank, then, no notice and opt out would be required because the bank is not using any eligibility information received from an affiliate to make the solicitation.

What if, in that same example, the bank provides its selection criteria to the mortgage company and the mortgage company uses its eligibility information to identify prospects for the bank and provides the bank with a list of names and addresses in order for the bank to make its own solicitations? Notice and opt out would be required since the bank is, in effect, using the affiliate's information to make a solicitation.

You can't avoid notice and opt out by using a service provider, such as a direct mail company, to make the solicitation for you. The regulations generally treat a service provider as the agent of the person on whose behalf it makes solicitations. A person is considered to have received and used eligibility information from an affiliate if a service provider acting on behalf of that person receives and uses information from an affiliate to make a solicitation.

In the case of service providers, the application of the new rules boils down to a question of who uses or controls the use of eligibility information and the actions of the service provider. In the example of a bank and affiliated mortgage company, if the mortgage company directs its service provider to use the mortgage company's eligibility information to market the bank's services and the bank does not control or communicate directly with the service provider regarding the use of the information, then the bank has not made a solicitation subject to the notice and opt out requirements. In order to avoid the notice and opt out, the affiliate providing the eligibility information must control the actions of the service provider who is sending out the marketing solicitation, not the person whose services are being marketed.

Special rules apply where eligibility information of a group of affiliated companies is maintained in a common database and a service provider, affiliated or not, has access to that information in order to send marketing solicitations on behalf of the various companies. In order to avoid the notice and opt out requirement, the affiliate whose eligibility information is being used must control its use by the service provider. There must be a written agreement between the affiliate whose information is to be used and the service provider giving the affiliate control over its use. The affiliate must establish the specific terms and conditions under which the service provider can access and use the information and those terms and conditions must be in writing. The affiliate must periodically evaluate the service provider's compliance with those terms. The affiliate must require the service provider to implement reasonable policies and procedures to ensure that eligibility information is used in accordance with the specified terms and conditions. Finally, the affiliate whose information is being used must be identified on or with the marketing materials, such as on an introductory letter or the envelope used to mail the materials.

If notice and an opt out opportunity is required, the notice must come from the affiliate that collected the eligibility information and that has the pre-existing business relationship with the consumer. In an affiliated group of companies, the notice can come from two or more, or all, members of the group as long as at least one has a pre-existing business relationship with the consumer.

The notice must be clear, conspicuous and concise and accurately disclose: (i) the name of the affiliate or group of affiliates providing the notice, (ii) a list of affiliates or types of affiliates covered by the notice, (iii) a general description of the types of eligibility information that may be used, (iv) that the consumer may elect to limit the use of the information to make solicitations, (v) that the election to limit use will last for the time specified in the notice (which must be at least five years), (vi) the consumer will be allowed to renew the election once that period expires, and (vii) provide a reasonable and

simple method for the consumer to opt out. A single opt out notice may be given to consumers on joint accounts, but either may elect to opt out. The notice must explain how an opt out direction for joint customers will be treated. An opt out direction may be treated as applying to all associated joint consumers or each joint consumer may be allowed to opt out separately. If each consumer may separately opt out, one joint consumer must be permitted to opt out for all, and all joint consumers must be permitted to make their election in a single response.

Model notices are provided in the regulation. The notice may be combined with privacy notices, and the agencies are working on a model, consolidated form for GLBA privacy, FCRA affiliate sharing, and FCRA affiliate marketing notices. However, you will want to consider carefully before combining affiliate marketing notices with annual privacy notices. Each opt out election made by a consumer will extend the opt out period for at least another five years.

A reasonable opportunity to opt out is given if the opt out notice is mailed and the consumer is given at least thirty days from the mailing of the notice to opt out by any reasonable means. If notice is given electronically, a reasonable opportunity to opt out may be given by posting the notice on the affiliate's web site where the consumer has actually obtained a product or service, the consumer acknowledges receipt of the notice, and the consumer is given at least thirty days after acknowledgment of receipt in which to opt out by any reasonable means. E-mail notice may be given if the consumer has agreed to receive disclosure by e-mail and the consumer is given at least thirty days after the e-mail is sent in which to opt out. A thirty day notice period is considered reasonable. A shorter period might be considered reasonable, but thirty days is a safe harbor under the rules.

Notice may also be given electronically at the time a consumer enters into an electronic transaction, such as on an Internet web site, where the consumer is required to make an election as a part of proceeding with the transaction and before the transaction is

completed. Similarly, in an in-person transaction, written notice can be given requiring the consumer to make an election before completing the transaction.

A reasonable and simple method of opting out includes a check-off box in a prominent position on the opt out form, a reply form and self addressed envelope included with the opt out notice, a toll-free telephone number to call, or by e-mail or some other electronic means where the consumer has agreed to electronic delivery of information. It would not be reasonable to require the consumer to write his own letter, to write or call and request a separate opt out form, to paper mail a reply when the notice is given electronically or to require going to a different Website without providing a link to that site. It is permissible to require consumers to opt out using a specific means as long as that means is reasonable and simple for that consumer.

The notice must be given in a fashion so that each consumer may be reasonably expected to actually receive it, although proof of receipt is not required. This may be accomplished by, for example, hand delivery of a printed copy, mailing a printed copy to the consumer's last known mailing address, e-mailing the notice to a consumer who has agreed to receive electronic disclosures by e-mail, or by posting the notice on a web site at which the consumer actually obtained a product or service electronically and requiring the consumer to acknowledge receipt.

The duration of the opt out must be at least five years and at the end of the opt out period, you may not use eligibility information from an affiliate to make a marketing solicitation to a consumer who previously opted out without giving the consumer a renewal notice and a reasonable opportunity to opt out along with a reasonable and simple method of doing so (and, of course, the consumer does not renew the opt out). The rules for content and delivery of renewal notices are basically the same as for the original notice, except that the renewal notice must also disclose that the consumer previously elected to limit use of certain information to make solicitations, the election has expired or is about to expire, the consumer may elect to

renew the election, the period of time a renewal election will apply, and that the consumer will be allowed at the end of that time to renew the election again. The renewal notice may be sent a reasonable time prior to the expiration of the existing opt out period and at any time after it expires, but no eligibility information received from an affiliate may be used to make a solicitation after the opt out period expires unless the renewal notice and opt out opportunity has been given and the consumer does not opt out.

Like all rules, there are exceptions. You may use eligibility information received from an affiliate: (i) to make a marketing solicitation to a consumer with whom you already have a pre-existing business relationship; (ii) to perform services on behalf of an affiliate (provided the affiliate is not barred from sending the solicitation itself as a result of a consumer opt out); (iii) in response to a communication initiated by the consumer about your products and services; (iv) with the consumer's consent or authorization; (v) if compliance with the affiliate marketing regulations would prevent you from complying with state insurance unfair discrimination laws; or (vi) to facilitate communication to persons for whose benefit you provide employee benefits or services under a contract with an employer arising out of an employment relationship or the consumer's status as a beneficiary under an employee benefit plan.

Of course, you can always use eligibility information collected from your own customers to make marketing solicitations on your own behalf to those consumers. Under the new rules, you can also use eligibility information obtained from an affiliate to make solicitations to your own consumer customers, those with whom you have a "pre-existing business relationship." A pre-existing business relationship is defined as a financial contract in force at the time a solicitation is sent, a purchase of a product or service (including holding an active account or another continuing relationship) at any time within eighteen months prior to making the solicitation, or an inquiry or application regarding a product or service any time within

three months prior to making a solicitation. Examples are provided for what constitutes an inquiry about a product or service. For example, a call to a branch or call center to ask about locations or hours of operation is not an inquiry regarding a product or service. Similarly, a consumer's telephone call to a centralized call center for a group of affiliated companies to ask about the consumer's existing account with one of those companies does not constitute an inquiry to any affiliate other than the one holding the existing account.

You may also use information from an affiliate to respond to a communication from a consumer about your products or services, without triggering notice and an opt out and whether or not you already have a business relationship with the consumer. For example, a consumer with a deposit account calls the bank to ask about how to save and invest for a child's education without specifying a particular product. Information about a range of investment products offered by the bank or its affiliates may be responsive, and the bank, its affiliated broker/dealer or any other affiliate offering investment products responsive to the request may use eligibility information from the bank or any affiliate to make solicitations to the consumer that are responsive to the request. The solicitations must be responsive, though. An inquiry or request for information about one product or a particular type of product would not justify use of eligibility information from affiliates to send solicitations about different products or types of products without first giving notice and an opportunity to opt out.

The exception for using information from an affiliate with the consumer's consent or authorization applies in a similar fashion. The use of information is limited to the extent of the consent or authorization given by the consumer. For example, a consumer customer of a mortgage lender authorizes or requests information about homeowner's insurance from the lender's affiliated insurance agency. The insurance agency may use information obtained from the mortgage lender to make solicitations about homeowner's insurance without triggering notice and an opt out. However the

authorization does not extend to use of eligibility information from the mortgage company to make solicitation about other insurance products offered by the agency.

The consumer must be given a meaningful choice. You may not use pre-printed boiler plate language in account agreements, loan applications or other documents giving authorization to you or your affiliates to use eligibility, information from affiliates to make solicitations.

The basic concept of the new regulations is not difficult to understand, but the application of the rules and exceptions to particular situations may become complicated. If your goal is to avoid giving notice and an opt out opportunity to each consumer, a careful study of the rules and exceptions will be necessary, and it is likely you will have to revisit the rules often whenever a new marketing program or solicitation is planned. If you plan to routinely give the notice and opt out, then careful consideration should be given to the content of the notice, how best to deliver the notice through various channels, where to receive and how to process opt outs, how to prevent improper use of information about consumers who opt out, the duration of any opt outs, whether or not to limit the duration to a particular time or to make opt outs permanent, and how to handle renewal notices if opt outs are not permanent.

Consumer eligibility information contained in a shared database may present special programming issues in order to set up firewalls and prevent improper access and use where a consumer has opted out or where you choose not to give notice and an opt out. One good point to remember is that information already contained in a shared database prior to October 1, 2008, the mandatory compliance date, is not covered by the new rules. Remember also, however, that if the information in the shared database that you want to use is consumer report type information other than experience information, the existing

FCRA affiliate sharing rules will continue to prohibit the sharing of that information without notice to the consumer and an opt out opportunity.

<Cliff Harrison>

### **FEDERAL RESERVE BOARD AMENDS REGULATIONS TO PROVIDE DISCLOSURES IN ELECTRONIC FORM**

---

On October 1, 2000, the E-Sign Act became effective. That legislation contained special consumer notice and consent provisions. The E-Sign Act now permits financial institutions to provide any written disclosures that are required to be made to consumers in an electronic format, provided that the consumer consents to receipt of these disclosures electronically.

In early 2001, the Federal Reserve Board (the "Board") issued interim final rules to establish standards for electronic delivery of disclosures under Regulation B (Equal Credit Opportunity Act), Regulation E (Electronic Fund Transfer Act), Regulation M (the Consumer Leasing Act), Regulation Z (Truth-in-Lending Act) and Regulation DD (Truth-in-Savings Act).

In response to a number of comments, the Board lifted the initial mandatory compliance date of October 1, 2001, and opted to delay further action in order to allow electronic commerce and electronic disclosure practices to continue to develop.

After allowing sufficient time to elapse, the Board in April 2007, proposed amendments to these various regulations that: (1) withdrew portions of the 2001 interim rules that restated provisions of the E-Sign Act; (2) withdrew portions of the interim rules that imposed undue burdens on electronic banking and commerce and which were perceived as unnecessary for consumer protection; and (3) retained certain provisions of the interim rules that either provide regulatory relief or guidance regarding electronic disclosures.

The effective regulations deal with a wide range of products and services that financial institutions provide to their customers. These include loan products, deposit accounts, electronic services and lease transactions, as well as issues related to advertising and the taking of applications. It is impossible to detail each of these final regulations as they relate to these various products and services in newsletter format; however, the balance of this article will outline the Board's general approach in developing its set of final rules to further the use of electronic disclosures.

In the set of final rules, the Board takes the position that financial institutions should not be required to obtain a consumer's consent in order to provide advertising, application-related and account-related disclosures if the consumer accesses an advertisement or application which contains those disclosures in electronic form, such as at an internet website. While the Board saw no harm to consumers who apply or seek information online in eliminating the E-Sign Act consent procedures, it did see an undue burden on those same consumers who chose to use electronic banking services if they were required to go through a consent process.

However, the Board recognized that consumers will not want all disclosures provided electronically, e.g., adverse action notices. So a consumer's consent to receive disclosures electronically will still be required in certain instances.

For those transactions in which a consumer submits an application form using a home computer via a financial institution's website, the financial institution must provide the disclosures in electronic form with the application on the website in order to meet the requirements to provide disclosures in a timely manner. Mailing paper disclosures would not suffice in that situation.

By way of contrast, if a consumer submits an electronic application at a financial institution's office, perhaps using a terminal or a kiosk, paper disclosures could satisfy the timing and delivery requirements through the use of a printer. This

approach might be preferable since it would make the necessary disclosures in a form which the consumer could keep. Note, however, that paper disclosures might not be required in those situations and that electronic disclosures could still be given, with certain specific exceptions such as the notice regarding copies of appraisal reports under Regulation B. Since that disclosure must be given in a form the consumer can retain, a paper disclosure related to the right to receive an appraisal report would likely be required.

The final rules eliminate the requirement that financial institutions maintain disclosures posted on their websites for at least 90 days, which was the original proposal. The Board believes that the length of time a consumer might wish to review a disclosure could vary depending on the type of disclosure. The Board now expresses a general expectation that financial institutions will maintain disclosures on websites for a "reasonable" period of time (depending on the particular disclosure), so that consumers can access, review and retain those disclosures.

The affected regulations which impose disclosure requirements provide that those disclosures must be given in a "clear and conspicuous" manner. Obviously, consumers today can access these disclosures through a variety of devices (e.g., hand-held, etc.). The final rules provide that disclosures would satisfy the "clear and conspicuous" requirement if they would be clear and conspicuous when viewed on a typical home PC.

Likewise, the requirement to provide disclosures in a form that consumers can keep will be satisfied if the disclosures are provided in standard electronic format that can be downloaded and saved or printed on a typical home PC. In other settings, the financial institution could provide a printer that automatically prints the disclosures.

The Board has taken a practical approach in revising each of these regulations. It is obvious that the Board is trying to prevent regulation from hindering the further development of electronic banking in all of its various forms.

Financial institutions that presently have electronic banking services or are considering offering such services should carefully review the details of each of these regulations to be certain that their electronic disclosure and other applications comply with these new final rules.

The mandatory compliance date for each of these revised regulations is October 1, 2008.

<Ed Wilmesherr>

### **GOOD NEWS AND BAD NEWS REGARDING BSA**

---

First the good news, FinCEN, on January 25, 2008, issued an administrative ruling to clarify the Currency Transaction Report (CTR) filing obligations when reporting transactions that involve sole proprietorships. The classification of sole proprietorship includes legal entities that operate under a "DBA" name. This new ruling (FIN-2008-R001) replaces FIN-2006-R003.

Under the new administrative ruling, financial institutions are only required to complete one section "A" of the CTR form, containing the name of the sole proprietorship's owner, the sole proprietorship's DBA name, the owner's social security number, home address, date of birth and occupation. Only the one section "A" is required, even if business operations have a different address and/or tax identification number than its owner.

FinCEN was careful to point out that it would continue to accept CTRs completed with two section "A"s when the transactions involve a sole proprietorship; however, hopefully this clarification will help to avoid a source of errors.

And now the bad news. Apparently the Justice Department is poised to impose its largest single monetary fine against a money services business in connection with yet another deferred prosecution agreement. This monetary penalty approximates \$25 M and stems from a failure on the part of the money services business to do an effective job of uncovering the full extent of the money laundering operation, despite having

filed suspicious activity reports in connection with the unusual activity detected.

We have related to you some of the details of the AmSouth deferred prosecution agreement and \$50 M fine. If you recall all of those facts, you will remember that there was more to the AmSouth situation than simply failing to file suspicious activity reports. Something about this money services business case seems to have some of those same overtones.

Nevertheless, numerous people who are familiar with BSA enforcement actions are offering the opinion that this action signifies a decision on the part of the Justice Department to raise the bar in terms of the requirements it will impose on financial institutions to investigate and dig further into the circumstances of transactions that are the subject of an SAR. If in fact that is the case, then a new level of compliance burden has been imposed. For now, banks should be cautious in the preparation and reporting of Suspicious Activity Reports and may want to err on the side of caution when it comes to performing a thorough investigation if a pattern of suspicious activity is detected.

<Ed Wilmesherr>

### **INTERAGENCY STATEMENT ON PANDEMIC PLANNING**

---

Just imagine. A strain of influenza infects millions spreading around the world. The first wave hits in late spring and summer. A second, much more severe outbreak occurs in the fall. A third wave occurs the following spring. Cities are quarantined. Hospitals are overwhelmed. Mail goes undelivered. Garbage goes uncollected. Businesses, schools, theaters, even churches are all closed. Community centers and schools are transformed into emergency hospitals but lack doctors and nurses to staff them. Deaths begin to mount, so much so that morgues and funeral operators run out of space. Not very likely to happen you say. Well, it already has. The Spanish Flu epidemics of 1918-1919 left 20 million dead around the world. In America, about 675,000 died. More

Americans died from the flu epidemics than were killed in World War I.

In December, the FFIEC agencies jointly issued an Interagency Statement on Pandemic Planning reminding financial institutions that business continuity plans should address the threat of a pandemic influenza outbreak and its impact on delivery of critical financial services. The guidance supplements the Interagency Advisory on Influenza Pandemic Preparedness issued in 2006 by the Fed, OCC, FDIC and OTS. Specifically, the guidance states that an institution's business continuity plan (BCP) should address pandemics and provide for a preventive program, a documented strategy for responding scaled to the stages of a pandemic, a comprehensive framework to ensure continuance of critical operations, a testing program, and an oversight program to ensure the plan is reviewed and updated.

The current threat originates from outbreaks of Asian flu in Asia. While there has been no sustained human to human transmission, the widespread nature of the virus in birds and the possibility of mutation over time increasing transmission among humans, raises the risk of a potentially disastrous outbreak.

The guidance points out that pandemic planning is quite different from traditional business continuity planning in which financial institutions plan for possible man-made or natural disasters. Those types of disasters may be relatively short in duration and confined to specific locations. Pandemic planning presents different challenges because the duration of a pandemic would be expected to be much longer, the impact more and widespread not limited to a particular location or geography. Pandemics generally occur in multiple waves, each lasting two to three months, and the impact will be widespread affecting not only the bank but its service providers including data processors, suppliers, off-site recovery systems, etc. Experts predict that the most significant challenge may be staffing shortage due to absenteeism. Employees may be ill, staying home for fear of becoming ill or to care for family members or

tend to children whose schools or daycares may be closed.

Pandemic plans need to reflect the institution's size, complexity and business activities. The potential impact of a pandemic on the delivery of the institutions critical financial services should be incorporated into the ongoing business impact analysis and risk assessment processes. The impact analysis should assess and prioritize essential business functions that might be affected, identify the potential impact of a pandemic on essential functions and processes; identify the potential impact on customers and the local economy; identify legal and regulatory requirements of the institution's business functions, estimate maximum downtime that might occur, assess cross training for key positions and functions, and evaluate the plans of critical service providers. The Department of Homeland Security provides a list of twelve planning assumptions that institutions should consider when developing the impact analysis.

To address the risks identified, the institution's BCP should provide for:

- A preventive program including monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers and provide appropriate hygiene training and tools to employees.
- A documented strategy for scaling the institution's response efforts consistent with the particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas, first cases in the U.S. and first cases within the organization. The U.S. government uses a six stage scale with a geographic focus (find it at [www.pandemicflu.gov](http://www.pandemicflu.gov)). The strategy should include plans on how to recover from a pandemic wave and preparation for any following wave.
- A comprehensive framework of facilities, systems or procedures to help provide the capability to continue critical operations in the event large numbers of staff are out for prolonged periods. Procedures may include things such as social distancing to minimize

staff contacts, telecommuting, directing customers to ATM's and online banking services, or conducting operations from alternative sites. The framework should consider the potential demand for and availability of communication services and increased reliance on telephone support services, online banking, ATMs and other similar electronic services as well as possible public health or government actions that may affect critical business functions.

- A testing program to help ensure practices are effective.
- An oversight program to ensure ongoing review and update of the plan.

An institution's board of directors is responsible for overseeing the development of the plan, approving the plan and ensuring that management has sufficient resources for planning, monitoring and testing. Senior management is responsible for developing the pandemic plan and translating the plan into specific policies, processes, and procedures, as well as for communicating the plan to employees and ensuring they understand their roles and responsibilities. Senior management is also responsible for being sure the plan is regularly tested.

The guidance identifies additional risk assessment and risk management strategies for institutions to follow in the planning process. It also lists sources of information including documents and websites covering pandemic planning, actions that might be taken to help prevent the spread of disease during an outbreak and checklists for governments, schools, businesses and homes. Regulators have said they will start checking during examinations to see if institutions are taking the threat seriously and are preparing for a pandemic.

<Cliff Harrison>

## **MRCG FEBRUARY MEETING TO BE HELD ON FEBRUARY 14, 2008**

The MRCG will hold its Quarterly Meeting on February 14, 2008, at the **Mississippi Sports Hall of Fame & Museum Conference Center, 1152 Lakeland Drive, Jackson, Mississippi**. Registration will begin at 9:00 a.m. with the Quarterly Meeting to begin promptly at 9:30 a.m..

During the February Quarterly Meeting, we will combine a series of topics into a discussion of the likely impact of the current credit crunch/mortgage crisis on the banking industry. One primary focus will be the newly proposed HOEPA regulations and a draft comment letter that the MRCG steering committee has requested. Those discussions will be followed by a review of the newly finalized Red Flag Guidelines and Affiliate Marketing Rules issued under the FACT Act. A series of brief compliance-related topics will be covered during the lunch hour, along with a presentation on Pandemic Flu preparedness.

As always, the dress code for this occasion is casual, and lunch will be provided. We ask that you fax or e-mail your registration form enclosed with this copy of the *Quarterly Report* to Liz Crabtree no later than **February 11, 2008** so that arrangements for lunch can be finalized. We look forward to seeing you there.

<Ed Wilmesherr>

**MRCG COMPLIANCE CALENDAR**

<b>1/31/05</b> - Revised FACT Act Notices Effective	<b>11/1/06</b> - EPA All Appropriate Inquiries Rule effective
<b>3/29/05</b> - Effective Date for Interagency Guidance on Response Programs for Unauthorized Access to Customer Information	<b>1/1/07</b> - Mandatory compliance date for Reg. E changes on electronic check conversions, payroll card accounts and ATM surcharge disclosures
<b>4/8/05</b> - Effective date for OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices	<b>7/1/07</b> - Reg E Payroll Card Account Provision effective
<b>4/26/05</b> - Joint Guidance on Banking Services to MSB's Issued	<b>10/01/07</b> - National Defense Authorization Act Usury Provisions Effective
<b>7/1/05</b> - Final Rule on Disposal of Consumer Information (FACT Act) effective	<b>1/1/08</b> – FACT Act Affiliate Marketing Rule Effective
<b>7/1/05</b> - Effective Date for Joint Guidance for Disposal of Consumer Information	<b>2/14/08</b> – MRCG February Quarterly Meeting
<b>8/1/05</b> -Disclosures re: Opt Out Rights for Credit Or Insurance (FACT Act) Final	<b>4/17/08</b> – MRCG Steering Committee Meeting
<b>9/01/05</b> - CRA Final Rule Becomes Effective	<b>5/15/08</b> – MRCG May Quarterly Meeting
<b>2/13/06</b> - OFAC Guidelines effective	<b>7/17/08</b> – MRCG Steering Committee Meeting
<b>4/1/06</b> - Deposit insurance limits on retirement accounts increased to \$250,000	<b>8/21/08</b> – MRCG August Quarterly Meeting
<b>4/1/06</b> - Effective date for FACT Act regulations on use of medical information in determining credit eligibility	<b>9/18/08</b> – MRCG Steering Committee Meeting
<b>5/22/06</b> - Comments due on information request relating to guidelines on accuracy of consumer report information and reinvestigation of disputes	<b>10/1/08</b> – FACT Act Affiliate Marketing Rule Mandatory Compliance Deadline
<b>6/30/2006</b> - Effective date for use of new SFHD forms	<b>10/1/08</b> – Electronic Disclosure Regulation effective
<b>7/1/06</b> - Effective date for Reg. CC amendments on remotely created checks	<b>11/1/08</b> – Red Flag Guidelines Compliance Mandatory
<b>7/1/06</b> - Reg. DD Amendments on Overdraft Privilege Plans Effective	<b>11/20/08</b> – MRCG November Annual Meeting