

ComplianceAction

VOLUME 13

YOUR SOURCE FOR REGULATORY COMPLIANCE

NUMBER 8

EDITOR

LUCY GRIFFIN

BOARD OF ADVISORS

JOHN J. BYRNE
 ROBERT P. CHAMNESS
 CLIFF E. COOK
 PHILLIPS G. GAY, JR.
 BARBARA E. HURST
 RICHARD INSLEY
 MICHAEL D. MAHER
 ROBERT G. ROWE, III
 ANDY ZA VOINA

What's INSIDE

Your Red Flag Program: Preventing Identity Theft (5 Action Steps) 3

Checklist for Developing a Red Flag Identity Program 4

Compliance Notes
 Common Violations; Victim Brokers? 5

Compliance Calendar 5

In the Editor's Opinion
 Risk Management and Common Violations 6

Compliance Notes
 Rentschler Receives Service Award; Bair Stresses Importance of Compliance; CAC Nominations ... 6

Compliance Q&A
 Funds Deposited Prior to Rescission Period; Flood Insurance Estimates on GFE; Denial of Credit for Length of Employment 7

Lowering the Threshold for the Travel Rule 8

Compliance Online 8

ComplianceAction

COMPLIANCE ACTION™ (ISSN 1085-326X) is published 16 times/year. Copyright © 2008 by ComplianceAction. Quotation by permission only. This issue went to press on June 26, 2008.

Credit Card Practices

The FRB Proposal

The lead topic discussed at the Federal Reserve Board's Consumer Advisory Council June 2008 meeting was the issues involved in the proposal on credit card practices.

Use of UDAP

A central concern for industry representatives is the fact that the proposal is based on the FTC Act's prohibition of unfair or deceptive acts or practices (UDAP). The proposal states a finding that the practices addressed are by their nature unfair or deceptive.

Another industry concern about this treatment is that the FTC does not plan to issue a similar rule for credit card issuers under its jurisdiction. Already facing statutory liability by applying UDAP, financial institutions would be at a competitive disadvantage.

If a practice is unfair or deceptive, it does not matter whether there is a rule in existence finding the practice unfair or deceptive. It is the nature of the practice that establishes

the status. The primary impact that such a rule would have is to save the plaintiff the legal challenge of proving that the practice was unfair to or deceived consumers. In the industry's views, this increased the ability of consumers to sue.

Several CAC members pointed out that the credit card practices could be dealt with under Truth in Lending's Regulation Z without taking the step of making a finding of unfairness or deception. By using UDAP authority, the rule covers debit cards as well as credit cards.

Some members observed that the proposal does not actually create a new standard or new liability. That already exists through enforcement actions and lawsuits brought by state attorneys general. However, the proposed rule would set a standard and clarify how UDAP would be applied.

(continued on next page)

ActionSteps

- ✓ **Review recent marketing material from the perspective of a consumer. How much can a reasonable consumer really understand about the product?**
- ✓ **Learn when and how rates are reset. Look at the resets from two perspectives: the credit agreement with the consumer and the possibility of disparate treatment.**
- ✓ **Determine whether your institution offers any programs that finance fees. Look at what consumers are targeted for these programs and how much credit is actually available.**
- ✓ **Review disclosures, both new account and change in terms. Read them the way a consumer would.**

Payment Schedules

The proposal would require credit card issuers to provide a 21-day period for payment by the consumer. Several CAC members questioned whether it is necessary to have such a lengthy period for payment in the context of e-payments and automatic transfers. Industry members opined that the payment period is an issue that is now passe.

Consumer advocates were not persuaded. Low- and moderate-income customers are more likely to pay by paper than electronically. A rule based on e-banking practices could have a disproportionately negative impact on the customers who most need protection.

The critical issue for consumers is that they receive the statement using a cycle that allows the consumer to make timely payment. The cycle, according to consumers, should account for postal service in both directions and adequate time – accounting for personal schedules – for the consumer to make the payment.

Allocation of Payments

The proposal offered three different methods for allocating payments. Each method was designed to ensure that the creditor honored any promises of low APRs. When creditors promise a low introductory rate or a low rate for balance transfers, consumers assume that the rate will be in effect for the period of time stated in the promotion; not dropped as soon as that balance is paid off by allocating all payments to the low rate balance. Methods in the proposal include payment of high-rate balances first and proportional allocation of payments to each balance under different rates.

This discussion opened the issue of whether the proposed rules would be more effective – and fairer – if made a part of Regulation Z rather than UDAP. A Federal Reserve rule under UDAP authority would affect only depository institutions while a rule issued under TILA would apply to all creditors.

Several industry representatives on the Council objected to the proposal arguing that any change in

how payments are allocated to balances will affect revenue. Losses in revenue will simply cause increases in other fees.

Aggressive – and sometimes misleading – marketing is what led to the concern about payment allocations. Several members of the Council commented on the difficulty in understanding advertisements. One member pointed out that, while all required information may actually have been included in the marketing material, the techniques of using different type sizes and colors actually obscure information that is important for the consumer to understand.

Industry representatives were also concerned about implementation and the changes required for systems. They asked that the Fed provide sufficient time to adapt systems. When consumer representatives suggested that it should not take two years to redesign systems, Anna Rentschler diplomatically pointed out that this is one system need among many, and recited several other system change demands important to consumers. “It is this with everything else” that calls for an adequate implementation period.

Rate Increases on Existing Balances

Generally, when a consumer borrows money, the consumer does so at an agreed-upon rate or a formula for setting the rate. In addition, consumers expect that, if they fail to make timely and adequate payments, the creditor may increase the rate. It has become a fairly common practice for credit card issuers to re-price consumer accounts based on aspects of the consumer’s behavior that have no direct relationship with the card issuer. Creditors use consumer reports to analyze risk and then reset rates according to the risk analysis. A consumer’s rate may therefore increase because of a late payment made to a third party.

Again, several of the industry representatives on the Council defended the practice while consumer representatives criticized the practice as unfair. The industry members advised the Federal Reserve that it should not limit the ability of banks to identify and manage risk. Repricing is

based on analysis of risk that may not have been present when the account was opened. Unlike closed-end credit when the entire risk analysis must be made at the beginning of the relationship, creditors can monitor and adjust risk for open-end programs.

Consumer advocates argued that this is fundamentally an unfair practice, leaving consumer’s with little ability to manage their credit. A consumer holding six credit cards might do or fail to do something that triggers a rate increase by all or most of the credit card issuers. One problem; six consequences.

One industry representative argued that consumers have plenty of choices and that this is entirely under the consumer’s control. Another member retorted that this argument doesn’t work unless and until credit scores are entirely transparent. Consumers have no way of knowing that an action in one area can affect their credit score and be used adversely by a different creditor.

Financing Fees

Credit programs designed to provide credit to high-risk customers can backfire by creating instant debt. Programs that have low credit limits, because of the consumer’s risk, often charge finance fees for membership or to secure the account. In some cases, this leaves the consumer with debt to pay and very little available credit.

Alan White, Assistant Professor at Valparaiso University Law School, described these credit programs as “promiscuously granted credit.” He also pointed out that this is low-documentation credit and implied that it should be looked at under the same microscope through which regulators are currently looking a low-doc mortgages.

Another member compared these credit card programs to FDIC’s small loan program, suggesting that some of the same controls should be in place.

The core question is whether such products are good for consumers, or actually do harm, placing the consumer in a worse position.

Preventing Identity Theft

Much of this summer's efforts will be spent on developing and implementing a red flag program for preventing identity theft. In developing such a program, the questions range from "what is it" to "how much is enough?" The biggest challenge to the program may be that it must be designed to monitor a moving target.

Identity theft prevention and information security are basically two facets of the same stone. The session on Information Security at ABA's National Regulatory Compliance Conference provided some sound advice for ID Red Flag programs together with information security.

Change

Rick Fischer, long recognized as the guru of privacy law, advised compliance managers to recognize that requirements change regularly. In his years of work with privacy laws, he can vouch for the fact that, especially in recent years, nothing stays still for long.

The program must be fluid to address a moving target. The rule places responsibility on financial institutions to anticipate techniques for identity theft and to identify ways in which the institution's systems may be vulnerable. You cannot design and implement a program based only on the agencies' red flag list and then sit back.

Risks change almost daily. Fischer recommends program reviews at least quarterly. In high risk areas and markets, the reviews should occur more frequently. As new risks are identified, incorporate the risk into your program and address it.

Another speaker recommended that you learn from past problems – yours and others. Experience is always a valuable teacher. And while criminals keep inventing new ways to commit crimes, especially on the Internet, they also never seem to let go of old tricks. And never rely on the agencies' list – that is the last place that a problem will be posted.

Theft Magnets

Thieves are after information so any information about consumers is a magnet. An essential first step in developing a Red Flag Program is to compile an inventory of all information about consumers. Determine where it is located. Determine the type of information. Determine the form in which the information exists. Consider any data, paper, e-mail, and don't forget laptops.

Your program should include shredding as an essential step once information has been used as intended. The easiest way to ensure compliance is to require shredding of all paper. Don't rely on staff to draw distinctions between information that is covered and information that is not.

Fischer advises compliance managers to focus on the information that will be the strongest magnet for identity thieves, such as account numbers. Any information that can be used for fraudulent transactions will be a magnet for thieves. Information sources such as drivers licenses can be used to create new accounts – one more good reason not to make copies for CIP purposes.

Information Inventory

The foundation of a red flag program is knowing where information is and how it can be accessed or compromised. This requires an institution-wide inventory of information. It's a little like Y2K or Privacy. Your inventory should include where the information sits – including where it might end up but shouldn't, who has access to the information, and where and how information might travel.

You also need to know how any information is protected. You might have the best firewalls available but if the information can be moved to a location outside of the firewall – have laptop, will travel and park in unsafe location – the firewall can't do its job.

Selling Management

As with many other programs, active involvement by management is essential. Part of your program development will be guiding management. It shouldn't be too difficult to grab management's attention: fear sells and you have lots of fear-based examples to use.

Program elements to consider could include designations of senior management responsibilities and assignment of a board member or board committee to be responsible for overseeing the program.

If the worst happens

If a breach should occur, have a plan for managing the response. How effectively you handle breaches can have everything to do with the institution's reputation going forward. Include steps, and even incentives, for identifying breaches and reporting them. Have a clear process for reporting breaches. Everyone in

(continued on page 8)

Action Steps

- ✓ **Determine where personal information is located and in what form.**
- ✓ **Set priorities based on the weakest or most vulnerable areas.**
- ✓ **Identify senior management who, based on their responsibilities and skills, would be appropriate for assignments of responsibility.**
- ✓ **Review vendor contracts and be sure that the vendor's responsibilities are clearly delineated and liability is allocated.**
- ✓ **Train everyone – including vendors.**

Checklist for Developing a Red Flag Identity Program

Because no two organizations are alike, everyone will have to develop their own Red Flag Program and each organization should have its own special issues. But there are certain basic steps that everyone will have to take. Below is a checklist of mandatory steps and considerations for developing your program. Adapt and add to this as appropriate for your circumstances.

Responsibilities	<input type="checkbox"/> Brief Board and senior management on program requirements. <input type="checkbox"/> Obtain assignment of responsibilities for development and oversight of program, including one or more members of the board and senior management.
Identify Accounts	<input type="checkbox"/> List a classification of all accounts by types and ownership. <input type="checkbox"/> Include both deposit accounts and loans. Include consumer accounts and business purpose accounts.
Identify Covered Accounts	<input type="checkbox"/> Identify all accounts or account types that have ownership or features that could be vulnerable to theft of a consumer's identity. <input type="checkbox"/> This may include accounts for small businesses, especially d.b.a. accounts.
Service Providers	<input type="checkbox"/> Review contracts and experience with all service providers. <input type="checkbox"/> Determine risk of each provider. <input type="checkbox"/> Review all contracts for required treatment of information security.
Estimate Risk	<input type="checkbox"/> Consider market risk, product risk, customer sophistication, and technical and procedural vulnerabilities.
Authenticating Customers	<input type="checkbox"/> Develop procedures and criteria for verifying customer identity for new accounts, transactions on existing accounts, and change requests.
Monitoring Transactions	<input type="checkbox"/> Develop procedures and protocols for monitoring transactions. <input type="checkbox"/> Include a reporting system for any suspicious activity or possible identity theft.
Customer Notifications	<input type="checkbox"/> For types of identity theft or risk of theft, determine when and how affected customers will be notified. <input type="checkbox"/> Determine what actions will be taken in response to possible theft, including consumer choices.
Consider Red Flags	<input type="checkbox"/> Use the list developed by the agencies. <input type="checkbox"/> Identify how information is vulnerable and ways that it could be accessed – e.g. shipping data, portable laptops, Internet access. <input type="checkbox"/> Monitor developments in information security, including information sharing with other institutions.
Set Schedules for	<input type="checkbox"/> Periodic review of covered accounts. <input type="checkbox"/> Periodic review and update of program. <input type="checkbox"/> Reporting.
Unscheduled updates	<input type="checkbox"/> Determine events that trigger review and updating, such as new products, system changes and trends in identity theft. <input type="checkbox"/> Assign responsibility for triggering review

Common Violations

At ABA's 2008 National Regulatory Compliance Conference, several regulatory agencies shared what they are finding as the most common violations. These violations are sufficiently common and costly that they should be regulars on your priority risk list. All agencies are finding flood violations, ranging from inaccurate determinations to incorrect insurance amounts. RESPA problems continue. It is not uncommon for examiners to find that there was no GFE or that the GFE was not timely.

A new area raised by the agencies was third party vendor management. This topic was addressed in the FDIC's recent FIL on managing third party risk. The message at the conference was consistent with the FIL: make sure that the vendor delivers the promised product or service in compliance with all the requirements.

The agencies indicated that improvements are needed in risk self-assessments. While they use the modern risk-assessment terminology, the example given by one panelist was identifying errors in HMDA data before the examiner arrives – a common violation.

The speakers also issued a warning about using off-the-shelf policies and procedures. No matter how carefully developed an off-the-shelf product is, it must still be adapted to how the institution operates. All policies and procedures should reflect the institution's real goals and procedures.

On the plus side, the agencies are seeing significant improvements in BSA compliance programs. They also noted – with pleasure – improvements in management involvement. In general, the agencies see these two areas as having positive trends.

Victim Brokers?

If you wonder what brokers are thinking, go to www.mortgagelawcentral.com Check the news for April 14, 2008. The story is about brokers suing lenders for ruining their reputations. After all, if the lenders didn't offer the product, the brokers wouldn't have sold it.

July

- * It is time to be working on affiliate sharing if you haven't already started. Begin by compiling categories of information, where it sits (your institution or a service provider) and affiliates with marketing ideas.
- * The Memphis check clearing office closes and the region's checks will be processed through Atlanta, beginning July 19, 2008. Check your list of local routing numbers.

August

- * Comments on the proposal for risk-based pricing notices are due to the Federal Reserve Board and FTC by August 18, 2008.
- * Comments on the proposal to reduce the \$3,000 threshold for the travel rule are due by August 21, 2008.
- * Look for final CRA Q&As late this summer.
- * Also watch for ID Theft Red Flag exam procedures late this summer or fall.

September

- * State member banks should put up the updated Fair Housing Lender Posters that show the new address for consumer complaints.

October

- * Schedule your annual training on fair lending and CIP. It's the anniversary month for both.

Coming Up Dates

- * The Identity Theft Red Flag program rule takes final effect on November 1, 2008.
- * Affiliate information sharing rules take final effect on October 1, 2008.
- * The Federal Reserve's Electronic Signature Rules for each regulation take final effect on October 1, 2008.
- * New Fair Housing Lender posters should be up no later than October 1, 2008.

In the editor's *Opinion*

Risk Management and Common Violations

Ten years ago – and even more recently – compliance managers used common violations as a management tool for setting priorities. If someone else had a problem with it, it could be a problem here. Common violations were and still are a good tool for tracking examiner priorities. If they find something, it means that they looked for it and if they looked for it once and found something, they'll look for it wherever they go.

Along came the four letter word: risk. Suddenly, risk was the tool. Compliance programs should be risk-based. Priorities should be set based on risk. Risk assessments should be conducted and repeated. The program should be adjusted and updated as risk changes.

What is the significance of this change? In fact, what's the difference between common violations and risk management? Does risk management mean that we no longer need to watch common violations? Or do common violations drive risk management?

Common violations stand for one of two things. A common violation is a requirement that is more likely than other requirements to have a violation. For example, finding and properly disclosing finance charges ranks high on the common violation list because it can be tricky to do correctly.

Or, the particular violation is easier to catch and therefore more common. Adverse action notices stand near the front of the line because they are a paper trail that is easy to follow. Either way, the examination citation exists.

When we use common violations as a guide, we direct our attention to the things that are most likely to go wrong. The common violations are a useful tool for targeting time and effort. Arguably, management by common violations is a form of risk management. Violations are a risk, and violations that happen more often than others represent a higher risk.

The question now, however, is whether common violations tell the entire story. Common violations are a useful tool because they are a measurement of symptoms. Historians will tell you that by learning from the past, we can anticipate and shape the future. This is what common violations do for us. They are a measure of what can go wrong and what did go wrong. Common violations are also a guidepost for finding how things went wrong.

But don't get too comfortable relying on common violations. Risk management is much more than management by common violations. It goes to the core of the business philosophy and how business gets done. Risk management measures the institution's commitment to compliance and safety and soundness. It measures its attitude toward its customers and its willingness to commit resources where needed. Risk management measures the balance between profit and integrity.

Common violations don't tell us the cause. When we find violations, common or otherwise, we have to figure out the cause. It isn't enough to fix the problem. Our question must be "how did this happen?" Determining how a problem happened involves looking at the practice from top to bottom. For example, if lenders are not properly identifying finance charges, is it because they don't know how to identify a finance charge? Or is it because they don't know how to use the software? Or is it because the message from above is "don't waste time on that?"

Risk management is therefore much more than counting violations and making notes to avoid them in the future. Risk management is a deeper look at the business – the dynamics and priorities of the organization.

So what do we do with common violations? Use them as an important tool in your risk management program. Use them to measure and benchmark, but be careful to look beyond at the bigger picture of business philosophy and practices.

Compliance *Notes*

Rentschler Receives Service Award

The 2008 Distinguished Service Award was presented to Anna Rentschler, BSA/AML Officer for Central Banccompany, of Missouri. In addition to her long record of banking work, Anna Rentschler has served as member and then chair of ABA's Compliance Executive Committee, is currently a member of ABA's Compliance Magazine board and has taught at ABA's national compliance schools. She is currently serving as a member of the Federal Reserve Board's Consumer Advisory Council where she ably represents the banking industry and compliance profession. Congratulations Anna!

Bair Stresses Importance of Compliance

If you were at ABA's National Regulatory Compliance Conference, you heard FDIC Chair Sheila Bair discuss the importance of compliance to financial institutions. In fact, she expressed concern that even regulators may not always give appropriate attention to compliance, particularly when safety and soundness concerns rise.

There were two themes to her luncheon speech. One was that the public needs to better understand the difference between depository institutions and the other players in mortgage lending. Bair herself has made herself heard on this topic in Congressional hearings. As a part of FDIC's 75th anniversary, the agency will stress this message.

Her other theme was the importance of sound underwriting. Responsible underwriting is essential for the banking business and for borrowers. Underwriting should be based on sound, documented information.

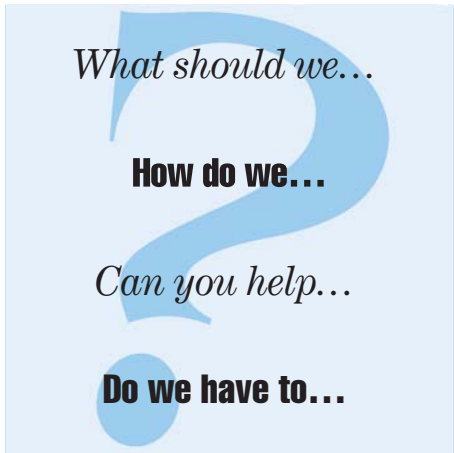
CAC Nominations

This is open season for nominations to the Consumer Advisory Council. Anyone can submit a nomination. Information on nominating is available on the Federal Reserve's web site. Nominations are due by August 24, 2008.

Question: We gave the applicant(s) the Right of Rescission notice and funds were accidentally deposited into their checking account before the rescission period was up. No harm was done to the customer, who did not know the funds were deposited until after the 3 day rescission period was up and they did not rescind the transaction. I know the consumers have 3 years to rescind if they do not receive the right to cancel doc at settlement, but would the 3-year rule apply in this case?

Answer: The short answer is “no.” You could have had a technical problem at the time, but that is now happily in the past. Let’s take a careful look at the regulation. In §226.23(a)(3), the regulation allows the consumer to exercise the right to rescind until midnight of the third business day following “consummation, delivery of the notice required by paragraph (b) of this section, or delivery of all material disclosures, whichever occurs last.” If the required notice or material disclosures are not delivered, the right to rescind shall expire three years after consummation...” This section lays out the situations that could extend the rescission period for three years. Early delivery of loan funds is not one of the reasons.

Now let’s look at the restrictions on disbursement. Section 226.23(c) prohibits disbursement until the consumer’s 3-day right to rescind has expired. The real purpose of this restriction is to protect the creditor. If the creditor disburses loan funds and the consumer rescinds, the creditor must first return all fees and costs to the consumer before collecting the disbursed funds. Under §226.23(d)(3), if “the creditor has delivered any money or property, the consumer may retain possession until the creditor has met its obligation under paragraph (d)(2) of this section. When the creditor has complied with that paragraph, the consumer shall tender the



money or property to the creditor or, where the latter would be impracticable or inequitable, tender its reasonable value...”

Question: I realize that the flood insurance premium should be disclosed on the good faith estimate and the HUD-1, but how do we come up with an estimate for this premium?

Answer: Good question. For the GFE, you will have to use a market estimate. This can be wildly inaccurate unless you know the flood hazard status of the property. When you come to prepare the HUD-1, there should be an actual number available – but you’ll have to ask the borrower what that number is since it is the borrower that purchases the insurance. On a more positive note, the flood insurance premium is going to be a p.o.c. item so you can write it in at settlement without changing any of the calculations or the numbers on page 1.

Question: Can you tell me if there has been a ruling or opinion about disclosing “length of employment” as a decline reason? I have seen a comment by a compliance officer that there was a “fair lending ruling” relating to potential discrimination against seasonal workers who can demonstrate consistent earnings, but I haven’t found the source.

Answer: Length of employment has been a fair lending concern for years. It pops up periodically and always in a different context and therefore sometimes with different answers. The context in which the factor is considered, and how rigidly the factor is used can also play a role. For example, judgmental consideration as long as it is fair, is less worrisome than considering the factor in a credit scoring system.

The basic position now is that length of employment can be considered and used as a reason for denial subject to conditions. Length of employment may be a credit-relevant factor. For example, a person who has only had a job for two months and has no other employment history presents risk that the lender may legitimately find unacceptable. However, a person with several years of consistent previous employment but two months on a new job presents a much lower risk. A third situation would be the individual who works on contract or on temporary jobs, such as construction. Counting their employment only for the period of time the applicant has worked on the present construction site fails to fully and fairly consider their employment history.

Contributing to the concerns in this situation is that the majority of persons who work under these employment situations are low- or moderate-income. They also disproportionately represent minority groups. Because of these concerns, lenders are advised to consider the applicant’s entire work history and not simply rely on the length of current employment.

To sum up, length of employment can be a legal reason for denying credit but the applicant’s length of employment should be considered in the context of the applicant’s complete employment history. Length and consistency of employment are the key elements to consider.

Enter the Vault

You've researched a topic, new or old, and read the regulation itself. Now you want an explanation of what all that meant, in practical terms. The BOL **InfoVault** is the central repository for articles & Q&As on topics from "Account Numbers" to the old "Y2K." Go to www.bankersonline.com/infovault/

PURPOSE:

To keep your compliance, audit, and legal officers and staff up-to-date on regulatory and compliance issues and industry related techniques;

To provide guidance for implementing and managing your compliance program;

To increase your awareness and understanding of compliance developments;

To provide you with information that will be useful in communicating compliance information to bank staff; and,

To assemble all of the above in a readable, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

Publisher

GEORGE B. MILNER, JR.
BANKERS INFORMATION NETWORK

Editor

LUCY GRIFFIN
COMPLIANCE RESOURCES, INC.

Subscription Rates:

To order or renew Compliance Action, call (800) 660.0080 or notify by mail at P.O. Box 1632, Doylestown, PA 18901, for a one year subscription at \$299. Letters to the Editor may be sent to the same address.

ComplianceAction is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that **ComplianceAction** is not engaged in rendering legal, accounting or other professional service. The information contained herein is intended to educate the reader and to provide guidelines. For legal or accounting advice, users are encouraged to consult appropriate legal or accounting professionals. Therefore, **ComplianceAction** will not be responsible for any consequences resulting from the use of any information contained herein.

Lowering the Threshold for the Travel Rule

FinCEN and the Federal Reserve have together published a request for comment on whether the \$3,000 threshold for the travel rule should be lowered or even eliminated. Law enforcement loves the information they can get from financial institutions. Every little bit is precious to investigators. And now they want more.

Law enforcement maintains that lowering the \$3,000 threshold would provide significant information for investigating financial crimes. For example, low as the \$3,000 threshold is, investigations have found situations where drug money is transferred in amounts under \$3,000 such as \$2,600 to \$2,900 and sometimes as low as \$500. In particular, human trafficking cases often involve low amount transfers.

One question the industry should raise is whether the additional work for institutions is really justified by what law enforcement might find. While law enforcement has established that money launderers can and do structure to avoid the \$3,000 recordkeeping, the fact is that law enforcement was still able to find those transfers and complete cases.

The proposal specifically asks law enforcement for additional information on the value of lowering the amount to trigger recordkeeping. Law enforcement is asked to explain the extent to which information about transfers of less than \$3,000 is valuable to investigations and to what extent investigations are hindered without such information. Law enforcement is also asked to explain how frequently they encounter cases with structuring under \$3,000 and whether the lack of information is a hindrance to those investigations. Finally, law enforcement is asked how frequently investigations would access such information.

For financial institutions, the question will be to what extent lowering the threshold would add burden. Comments should focus on cost and frequency of such transfers. The agencies are particularly interested in whether current technology has sufficiently reduced the burden of compliance to support lowering the threshold. Financial institutions should provide comments with specific cost breakdowns. It would also be helpful to describe when and how the required information is gathered.

One thing the industry should consider, in comments, is whether the additional information that would be available by lowering the threshold is important to the investigation or merely nice to have – with an easy way to get it.

Comments are due to either agency by August 21, 2008.

Your Red Flag Program: Preventing Identity Theft *(continued from page 3)*

the organization should know what to do and whom to contact – and that includes vendors.

Next, take control of the situation. Don't wait for your regulator or a customer to dictate your responses. Treat this as an opportunity to do something positive for your customers. No-one wants a breach, but a breach is also an opportunity to take decisive action.

The identification of a breach doesn't necessarily mean that the institution was careless. It can mean that the institution is alert and on top of things. Your communication with the consumer can state that, because you have a state of the art program, you have identified a possible breach and then advise the consumer how to work with you to prevent harm. In other words, take credit instead of blame – unless something really stupid actually happened.

The program could contain standards – admittedly theoretical – for when and how to notify your regulator. Some investigation is appropriate to be certain that there has been a breach. So calling immediately may not be necessary. But it is a good idea to have some standards in your program.

Final Advice

Rick Fischer pointed out that it is impossible to protect all information all of the time. Perfection is not possible. You should recognize that and instead deal with reality.