



Compliance News...

On Saturday, May 24, 2008, we had a fire at our office. This was not an exercise of our disaster recovery plan! Fortunately, most of our information is saved electronically and we had performed a backup two days earlier. If you click on the following link, you can see the fire was very devastating: <http://www.bankerscompliance.com/blog/office-fire.htm>

The fire was caused by a lightning strike resulting in an electrical surge. It started in an electrical box and was mostly contained in a wall and our ceiling. The picture at our website shows my desk. You can see ceiling rafters that fell on my desk and a light fixture (upper left corner - the "white thing"). Most of our office doesn't look this bad, but the heat melted printers, monitors, our 3 computers and bubbled the finish on the enamel/wood surface on every table, desk, book shelf, etc. If that didn't ruin everything, the smoke penetrated everything else and left soot that can't be cleaned.

Most damaging to me are the personal things (pictures of my wife and children, books, etc.), my FDIC regulations (15 years of notes!) and my seminar manuals (lots of information that can't be replaced). The good news: No one was hurt and the support of our community (both here in Central City and the banking community) has been tremendous. Unfortunately, sometimes we have to have disaster to see how great our friends really are. Unfortunately, most of the files on our hard drives were not retrievable. Even our back up system was damaged by the severe heat.

Since we have 5 consultants in 5 different cities, we were able to route calls and emails to them for the week following the fire. I believe some emails may have been lost in the shuffle and we went from three phone lines to one. Our email and phone/fax lines have all been restored. If we didn't respond to you by now (for submitted emails), please re-send your email. If you received a busy signal, I apologize for your inconvenience. Thanks for being patient with us while we recover.

Dave Dickinson

FACT Act Deadlines Quickly Approaching . . .

It's hard to believe that June is already here and that means October and November will get here faster than you may think. So why should you be concerned about October and November? These are the months in which compliance with the Fair and Accurate Credit Transactions (FACT) Act's Affiliate Marketing, Red Flags Identity Theft and Address Discrepancy provisions become mandatory. October 1, 2008, (Affiliate Marketing) and November 1, 2008, (Red Flag Identity Theft and Address Discrepancies) are the magical dates. Each of these requirements is going to take a lot of thought and planning prior to being implemented and in the case of the Red Flags Identity Theft provisions, approved by the Board of Directors. That's why it is imperative you start working on these requirements now.

We have devoted the entire June Newsletter to the FACT Act. We have developed a sample [Red Flags Identity Theft Policy and Procedures](#)¹ to help get you started. However, it is important that you don't just copy the Policy and Procedures. This is because one of the important pieces of these provisions is to make it "fit" YOUR institution. You may need to add more examples or remove some that do not apply to your institution. We have also included a suggested timeline for implementing these provisions (see below). Finally, we have included a Question & Answer on these topics generated from seminars we conducted.

For a quick recap of what these provisions require, check out our [January](#)² and [February](#)³ newsletters as well as our [blog](#)⁴.

Don't let time slip away!

¹ <http://www.bankerscompliance.com/assets/files/documentation/FACT%20Policy%20&%20Procedures.doc>

² http://www.bankerscompliance.com/assets/files/newsletters/2008/January_2008.pdf

³ http://www.bankerscompliance.com/assets/files/newsletters/2008/February_2008.pdf

⁴ <http://www.bankerscompliance.com/blog/fact-act-red-flags-and-address-discrepancies.htm>

Red Flags Identity Theft Implementation Timeline . . .

FACT Act Identity Theft Prevention Program Implementation Timeline	
June 2008	Review the sample policy and procedures developed by Banker's Compliance Consulting. The Bank should customize the policy and procedures to fit its profile and level of complexity. Have the Board of Directors approve the ID Theft Prevention Program (policy and procedures).
July 2008	Provide training to all applicable employees. Implement the program after training is completed.
July 2008 to December 2008	The Bank will need to monitor its compliance with the program requirements. Additional training and increased ongoing monitoring may be required based on the level of compliance with the program requirements.
January 2009	Submit the required annual report to the Board of Directors.

Upcoming Seminars – Mark These Dates . . .

We will be conducting our **Advanced Deposit Operations and Advanced Lending Compliance Seminars** this fall. These seminars are always very well attended. For your convenience, you can register and pay by credit card on our website: <http://www.bankerscompliance.com/products/>

The dates and locations are as follows:

August 19 – 21 – Grand Island, NE

September 9 – 11 – Sioux Falls, SD

October 21 – 23 – Omaha, NE

Banker's Compliance Consulting Q & A Forum...

The following Q & A's were generated our FACT Act Seminars.

FACT Act Compliance Seminar Questions and Answers

Identity Theft Red Flags – Risk Assessment/Applicability

Question 1. When documenting the bank's risk assessment, would it be sufficient to have, at a minimum, a statement of "All accounts at this institution are considered covered accounts and all Red Flags will apply"?

Answer: Yes.

Question 2. Does the FACT Act apply to dealer loans?

Answer: Yes.

Identity Theft Red Flags – Written Program & Board Approval

Question 3. On page 22 it states that the written program must be approved by the Board of Directors or an appropriate committee of the Board. We have a compliance audit committee, would they be able to approve the written program?

Answer: We feel that if the Board of Directors formally recognizes the Audit Committee for such purposes, this would be sufficient. The Audit Committee should still provide an executive summary to the Board of Directors for review.

Question 4. Can the Board of Directors simply review the ID Theft procedures?

Answer: This Law states the Board must approve the "initial" program which, technically, is the policy and procedures. It does allow for changes to the procedures without Board approval. In fact the preamble states, "The final rule continues to require approval of the written Program by the board of directors or an appropriate committee of the board. However, to ensure that this requirement does not hamper the ability of a financial institution or creditor to update its Program in a timely manner, the final rules provide that the board or an appropriate committee must approve only the initial written Program. Thereafter, at the discretion of the covered entity, the board, a committee, or senior management may update the Program."

Question 5. Regarding the periodic updates to the Identity Theft Program, would a verbal report to the Board of Directors be sufficient?

Answer: Nowhere in the Law does it state that the updates must be approved by the Board. However, we still suggest documenting the updates either by having the Board re-approve the Program or addressing the update report in the Board minutes. We don't think examiners will buy that you really provided a verbal report with no documentation.

Question 6. Does a bank need a separate policy and procedures for the Red Flags and the Address Discrepancy rules?

Question 7. Does addressing Address Discrepancies need to be in the procedures?

Answer: Written policy and procedures are only required for the Red Flags/Address Discrepancy rules that take effect later this year. Address Discrepancies are actually one of the many Red Flags. The most common indicator of identity theft is address discrepancies so additional emphasis was focused on this area. A bank can have one policy to address both. However, the procedures particular to an address discrepancy may need to be expanded.

Question 8. Several participants indicated there were no specific procedures regarding address discrepancies in the sample procedures provided.

Answer: An address discrepancy is a red flag and although the regulation provides three very specific options for responding, each response includes “contacting the customer”. Therefore, we feel the procedure #2 in Section III, Responding to Red Flags, in the sample procedures address all three of the following regulatory options. However, you may wish to be more specific in your own procedures.

- Notify the cardholder at their former address and allow the cardholder to promptly confirm an incorrect address;
- Notify the cardholder of the address change request by another means of communication previously agreed to by the issuer and the cardholder; or
- Use other reasonable means of evaluating the validity of the address change

Question 9. Does management need to notify the Board of each particular Red Flag incident?

Answer: No, addressing a summary of the Red Flags during the annual review will be fine.

Question 10. Are there different procedures for ID theft that need to be addressed for loan renewals and for opening accounts for existing customers as opposed to opening loans and new accounts for new customers. We have a relatively small customer base and most of the time we know our customers that walk in the door.

Answer: You will need to tailor your procedures to fit your bank. Obviously, with existing customers you know more about them (for example, their financial habits). So, you may be able to detect/prevent identity theft easier than for a new account. For new accounts, you will have CIP requirements to assist you in identifying potential identity theft at the time of account opening, as well.

Question 11. We are planning to open an online branch soon, which will not have any signature cards or face to face contact. Are there different ID theft procedures that we will need to address for this area? We are already planning to ask several ID questions as well as out of wallet questions to help insure that the person is who they claim to be.

Answer: When opening new accounts, you will utilize your CIP procedures to detect identity theft. You may need to incorporate some additional Red Flags in your procedures to encompass these online accounts.

Question 12. We periodically receive emails from VISA called “CAMS” reports that give us our customers VISA card numbers that could possibly be compromised in some manner. Do you agree that this would be classified a “red flag” for the Identity Theft Program?

Answer: Absolutely. This sounds like an excellent tool for detecting potential identity theft.

Question 13. Are we required to perform independent testing for Section 114 (Red Flags/Address Discrepancies) at regular intervals?

Question 14. Does Section 114 of the FACT Act (Red Flags & Address Discrepancies) require independent testing? Are we required to sample new accounts and loans for compliance on an annual basis?

Answer: Nowhere in this Section of the FACT Act does it require independent testing. While this may be a good practice to ensure your bank’s compliance with the requirements, it is not required by law. However, you will need to monitor your compliance in some manner so you ensure you are in compliance and so you can report your compliance with these requirements to your Board.

Identity Theft Red Flags - Service Provider Due Diligence

Question 15. Who qualifies as a Service Provider for the ID Theft Program? I understood you to say only parties involved in our ID Theft prevention or ID Authentication would qualify. I am wondering if you have a reference point for that because as I understand the preamble information under "Section .90(b)(10) Service Provider", they are defined per Information Security Standards (provided below). This additional statement also muddied the waters for me...."The Agencies have concluded that defining "service provider" to include only persons that have access to customer information would inappropriately narrow the coverage of the final rules."

Answer: The Information Security Standards define “service provider” to mean *any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through the provisions of services directly to the financial institution.* This definition basically encompasses every provider of the bank. You need to look at every third party relationship, such as, indirect lending, marketing, broker relationships, check orders, etc. Any “service provider” that maintains, processes or has access to consumer information should have policies and procedures to detect, prevent and mitigate identity theft.

Question 16. Once we determine which service providers qualify, I'm questioning the steps needed to confirm their commitment to ID Theft if it is not included in their original contract. Will we need a signed agreement similar to the Confidentiality Agreements in place for Privacy?

Answer: The final rule is very vague on this subject. The final rule states that a covered entity must “*exercise appropriate and effective oversight of service provider arrangements*” without further elaboration. This is to give financial institutions maximum flexibility in how they oversee their service providers. It goes on to state that a financial institution “*could require the service provider, by contract, to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider’s performance of the service provider’s activities and either report the Red Flags to the financial institution or take appropriate steps to prevent or mitigate identity theft.*” While this example is in the final rule, it is not required.

Question 17. Is Shazam considered a service provider when discussing the service provider due diligence requirement?

Answer: Yes. Shazam typically monitors your debit/credit card accounts on your behalf and generates various reports on suspicious activity or transactions.

Question 18. Our credit reporting agency checks for risk factors on credit reports before sending them on to us. Do we need to perform the due diligence for this service provider?

Question 19. What about ChexSystems/E-funds?

Answer: We feel there would be no due diligence required for the credit reporting agency since you obtain the reports directly from them. However, ChexSystems/E-funds may since you are relying on them to detect red flags with respect to deposit accounts.

Question 20. Have third party service providers come up with a way to show compliance with the FACT Act?

Answer: We are unaware of any set standards at this time.

Question 21. If we open accounts online and rely on a 3rd party to perform verification, what are we required to do?

Answer: The regulation requires you to perform due diligence of 3rd party service provider arrangements where you rely on the 3rd party for compliance with respect to the requirements of this regulation.

Question 22. Our bank has an agreement with a company to provide credit cards to our customers. We provide the customers with an application and then the other company does the underwriting and issues a card in our bank's name. Is the bank required to do diligence on this type of service provider?

Answer: If these credit cards are maintained on your bank's books, then we feel that you should perform due diligence requirements on this provider. However, if you are simply providing the application and receiving a fee to do so, then this would not appear to require additional due diligence.

Reporting/Documenting Identity Theft

Question 23. What is the proper documentation method when responding to a Red Flag?

Answer: A simple description of "yes, identity theft confirmed" or "no identity theft, acceptable reason for Red Flag". Beyond that the bank has no burden to resolve on customer's behalf.

Question 24. Relating to Page 23 in the seminar manual, specifically B (3) "What to do if the customer is not who they say they are", if an individual appears in person and you are certain there is something that is just not right, why not call the police?

Answer: We think your suggestion is a great idea. Each bank is free to determine when and if they will contact local law enforcement with regards to potential identity theft.

Question 25. Is there a central location to report ID Theft or to keep up on the latest ID Theft schemes?

Question 26. How does a bank educate its customers to understand the importance of protecting themselves from identity theft?

Question 27. How do we communicate the issue of identity theft to our customers? How much do they "need" to know?

Answer: There is no central place for bank to report ID Theft. However, the Fair Trade Commission's (FTC) website is an excellent resource for both a bank and their customers. It contains step by step instructions for victims of identity theft, forms, etc. It also has information on new trends in identity theft. We feel that educating your customer will potentially benefit the bank in the long run. You can access the website at: <http://www.ftc.gov/bcp/menus/consumer/data/idt.shtm>.

Additionally, <http://www.ftc.gov/idtheft/>

Question 28. Where do we report identity theft?

Answer: There is no set "contact list" for identity theft. If you are required to file a SAR, then you need to do so. Anytime fraud is involved, the Privacy Act is no longer a concern for the bank. Depending on the circumstances, you could contact local law enforcement, your state's Attorney General, or your state Department of Banking to report the identity theft.

Question 29. What if you alert the customer to potential identity theft and they do not want to take any steps to correct it?

Answer: If the identity theft affects the bank (a loan, deposit account, etc.) then the bank must comply with the requirements of the FACT Act. However, if the identity theft is discovered by the bank but does not affect any covered accounts, then the bank has no additional responsibility. If the customer does not want to pursue any course of action then that is their prerogative.

Question 30. Do we need to file a SAR when we encounter a Red Flag?

Question 31. Will the bank be required to file a SAR on Regulation E claims?

Answer: Identity theft is a category listed on the SAR form. If you suspect identity theft and it meets the reporting thresholds, then you must file a SAR. Be sure that you do not file a SAR on the victim of the identity theft. If you don't know who the perpetrator is, the filing threshold is \$25,000. Some banks have taken the stance that they will file a SAR anytime they have suspected identity theft regardless of the amount involved (this is not required by regulation).

Address Discrepancies

Question 32. Two different departments handle the address change and the issuing of credit cards. How do you recommend the two departments communicate?

Answer: The department issuing the credit cards may need to look at the CIF screen to see if there have been any updates in the last 30 days. Each bank will need to determine their procedures to facilitate communication when necessary.

Question 33. For resolving address discrepancies if you verify the customer address at the time of the card ordering (for example, verify their challenge questions etc) would that be sufficient?

Answer: Yes. However, if you receive an address change within 30 days you should still use some means to verify there is not potential identity theft.

Question 34. Is recognizing the customer's voice over the phone sufficient for resolving address discrepancies?

Question 35. Would we have to ask an identifying question or is voice recognition enough because we are a small bank and know most of our customers well? Would we have to outline what these questions will be? (Ex. If we ask them what their school nickname was and we don't know where they went to school, how would we know if they answered correctly?)

Answer: We realize that in small banks this may very well be the case. However, we feel that voice recognition is probably not the best address discrepancy resolution process. We would suggest implementing some other form of resolution, such as identifying questions. You should make sure the questions you ask are ones in which you know the correct answer and are "out of wallet" questions. One example might be "what is your monthly mortgage payment?"

Question 36. Where should we keep our documentation for resolving address discrepancies?

Answer: There is no regulatory answer to this question. You could keep a log (there is no requirement for a log in the law). You could keep the information by writing it on the credit report or debit card order form, etc. Stay tuned as we may find out more on this in the months to come.

Question 37. If you don't upload to a credit reporting agency, how can you correct an address discrepancy found on the credit report?

Question 38. Our bank utilizes credit reports when establishing a credit account or a deposit account. However, we only upload to the bureau on the credit side. If the bank encounters an address discrepancy on the deposit side, would we be required to upload the correct information?

Question 39. We currently use credit reports for all new customer deposit account openings, but we do not report deposit account information to the reporting agencies. Would we be excluded from the requirement to furnish discrepancy information because it is not part of our "ordinary course" of business?

Answer: If you don't upload, you have no responsibility to correct the address found on the credit report. If you only upload on the loan side but still use credit reports on the deposit side, you will only be required to verify that the credit report you pulled is for the customer. You will not have to report deposit address discrepancies since it is not your practice to upload on the deposit side.

Question 40. What if you type in the customer's physical address and the credit report has the P.O. Box address on file; is this considered an address discrepancy?

Answer: We don't think so. However, we would suggest documenting this somewhere. You might consider uploading the physical and P.O. Box addresses the next time you upload information to the credit reporting agency.

Question 41. I understand that we must verify the validity of an address change within 30 days of a request for a new card. Does the verification requirement apply to cards ordered by the bank (without customer request) to replace an outstanding card that will expire?

Question 42. Does the bank need to perform due diligence on expired cards prior to sending?

Question 43. It would seem that if we verify any address change requests when the request is received, we would not have to do another verification when a renewal debit card is sent. We often get mail back that we have sent out to customers with a post office sticker indicating that there has been an address change. Would it now be necessary to either call or write the customer to make certain that this address change is correct?

Answer: We believe that any address change followed by a new card (due to lost, stolen or expiration) within the next 30 days is an address discrepancy red flag. A card that will expire for example, you have a thief who knows your card is going to expire in July 2008 might call your bank and try submit an address change right before a new card is sent out. Additionally, notification from the post office of an address change followed by a new card would be considered an address discrepancy red flag.

Question 44. Would the same FACT Act address discrepancy rules apply when a customer is asking to replace a checkbook or periodic statement?

Answer: Yes, the same rules would apply. It would seem unlikely that an identity thief would request checks etc., to be printed at the issuing bank.

Question 45. When confirming address changes with our customers, would telephone call backs be sufficient?

Answer: A call back alone would not be sufficient as you may still be talking to the thief. We would recommend adding “out of wallet” challenge questions to the call back.

Question 46. When should address discrepancies be resolved?

Answer: Before an account is opened.

Question 47. Do the FACT Act address discrepancy rules apply to dealer loans?

Answer: The banker or dealer needs to resolve any discrepancies prior to closing the loan.

Question 48. A customer called to say they never received their credit card indicating they moved. The customer provides an updated address and a plastic will subsequently need to be sent. Does this situation fall under the rules?

Answer: Yes.

Question 49. Same as above only the person calls to state their card was lost or stolen. They also have an address change and require a new plastic. Does this situation fall under the rules?

Answer: Yes.

Question 50. The FACTA really isn't specific regarding the necessity of the customer to respond back to the letter that was sent advising them of the address change and plastic request. If we send the letter out and have had no response within 10 days, can we assume everything is fine, or are we required to wait for a response before the plastic is sent?

Answer: As you stated there is no guidance on this. However, we would not recommend assuming no response means everything is fine. You may want to implement other methods to contact the customer and verify the address change.

Question 51. The regulation only requires the letter to be sent to the old address. In the subprime industry many customers do not forward their mail to their new address. Do we have any requirements if the letter is sent back to us?

Answer: If the letter is returned, we would recommend some other means of verifying with the customer.

Question 52. Rather than sending the letter in some circumstances, we were questioning utilizing challenge questions when they called in for the plastic. The objective would be to verify their identity and then validate the address. Would this be acceptable as alternative policies and procedures?

Answer: We feel this would be acceptable.

Affiliate Marketing

Question 53. What about employees who have duties with both the bank and an affiliated company?

Question 54. We have a joint employee that works as a teller and also is an insurance agent in our drive through. How are we affected by the Affiliated Marketing Rules?

Answer: You cannot prevent someone from taking "knowledge" from one side to the other. However, that employee cannot take any lists, electronic information, etc. to assist them in their duties.

Question 55. Can a banker refer a customer directly to an affiliate (i.e. insurance company)?

Answer: A banker can refer and provide affiliate information to the customer. However, the banker cannot provide customer "eligibility information" to the affiliate so the affiliate can initiate the call.

Question 56. Can a bank reference its affiliates or provide brochures of its affiliates in a marketing letter to a customer?

Answer: Yes, as long as no customer "eligibility information" is shared to the affiliates a bank may provide affiliate information. However, keep in mind additional advertising rules may apply.

Question 57. We disclose in our Privacy Policy to our customers that we may disclose information for marketing purposes to non-affiliated third parties. The customer then has the option to "Opt Out". Our non-affiliated third party is a company that we sold our credit card portfolio to. When we signed the contract to sell our credit cards to them, they asked to be able to market our customers that do not presently have a credit card.

This is a non-affiliated third party that we do not employ and is not an affiliate of our bank. Do we need to do anything regarding the FACT Act regarding non-affiliated third parties?

Answer: No. The Privacy Act governs sharing with non-affiliates. The Fair Credit Reporting Act (FCRA) governs sharing “non-experience” information with affiliates. And the FACT Act governs sharing “non-experience” information with affiliates for marketing purposes only.

Question 58. What is an affiliate?

Answer: The following 3 definitions are all necessary to fully answer this question:

Affiliate means *Any company that is related by common ownership or common corporate control with another company.*

Company means *Any corporation, limited liability company, business trust, general or limited partnership, association or similar organization.*

Common ownership or common corporate control means *a relationship between two companies under which:*

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the Board determines; or

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i)-(i)(1)(iii) of this section.

Question 59. How do the affiliate marketing sharing rules apply with respect to holding company employees who conduct marketing on behalf of all affiliates?

Answer: We are not sure what your exact situation is; however, we will try to answer your question giving a couple different scenarios.

A bank can share “eligibility information” with a holding company employee to market the bank’s products to the bank’s customers. Sharing “eligibility information” with a holding company is not viewed as sharing for marketing purposes under this rule because a holding company does not typically have products to market. The key to this scenario is that the bank’s “eligibility information” is being used to market to the bank’s customers.

Another scenario would be a bank and an insurance company under the same holding company. The insurance company could forward marketing information to the holding company employee to market their products to bank customers. As long as the bank or holding company employee does not communicate to the insurance company who the information was sent to, this would not violate the FACT Act affiliate marketing rule.

Miscellaneous

Question 60. Do you need to go looking for Red Flags/identity theft on existing accounts, such as by routinely pulling credit reports?

Answer: You don't need to go looking for it but if something shows up during ordinary business you need to investigate.

Question 61. Since the FACT Act affects more than just banks, who regulates the other types of entities?

Answer: The Federal Trade Commission.

Question 62. How does a bank confirm if a social security number is legitimate?

Answer: You can visit www.ssn.gov. This has various references for when and where certain numbers were issued.

Question 63. Do we need to have policy and procedures for each section of the FACT Act?

Answer: A written policy and procedures are only required for the Red Flags/Address Discrepancy rules that take effect later this year. However, it might be a good idea to have written procedure for the other FACT Act sections merely as a means to keep all employees aware of what they are required to do.