

B&B REVIEW

Financial Services and Transactions

DEADLINE IS NOVEMBER 1, 2008 FOR BOARD-APPROVED I.D. THEFT PREVENTION PROGRAM

For Further Information Contact . . .

Jennifer R. McCain
205-226-8777
jmccain@balch.com

Matthew P. McLaughlin
601-965-8162
mmclaughlin@balch.com

Katharine F. Musso
205-226-8707
kfmusso@balch.com

W. Brad Neighbors
205-279-2940
wneighbors@balch.com

Michael D. Waters
205-226-8720
mwaters@balch.com

W. Clark Watson
205-226-3466
cwatson@balch.com

Lois S. Woodward
205-226-3478
lwoodward@balch.com

Stephen A. Yoder
205-226-8791
syoder@balch.com

Visit our website:
www.balch.com

For Address Changes, Contact:

Nora Yardley
205-488-3476
nyardley@balch.com

INTRODUCTION

Bank customer information security has been a top priority issue in Washington for nearly a decade. The Gramm-Leach-Bliley Act of 1999 required financial institutions to implement information security programs designed to protect their customers' information. The banking regulators responded in February 2001 with "guidelines" for information security programs generally. In August 2003, the regulators issued "guidance" setting forth the components of a response program for identity theft.

Responding to the surge in identity thefts, in December 2003 the President signed the Fair and Accurate Credit Transaction Act ("FACT Act"), which directed banking regulators to issue formal regulations and further guidelines for identity theft. The regulators issued proposed regulations for the FACT Act in July 2006, which were finalized in November 2007. The deadline date for a bank's final implementation of a written Identity Theft Prevention Program (a "program") described below is November 1, 2008.

Banks that have not already adopted a compliant program should be working one now to meet the November 1, 2008 deadline date.

INSTITUTIONS THAT MUST IMPLEMENT A PROGRAM

Any financial institution that offers or maintains one or more "covered accounts" must develop and implement a written program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Any bank that is in the consumer banking business is likely to have covered accounts requiring development of a program.

A "covered account" is (i) an account that a financial institution offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.

ELEMENTS OF A PROGRAM

An identity theft prevention program must include reasonable policies and procedures to:

- (1) Identify relevant "Red Flags" (see discussion below) for the covered accounts that the bank offers or maintains, and incorporate those Red Flags into its program;
- (2) Detect Red Flags that have been incorporated into the program;
- (3) Respond appropriately to any Red Flags that are detected in order to prevent and mitigate identity theft; and
- (4) Ensure the program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the bank from identity theft.

IDENTIFYING RED FLAGS

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

When identifying relevant Red Flags for covered accounts, a bank should consider several factors including the types of accounts it offers or maintains, the methods

Visit Our Offices...

1901 Sixth Avenue North
Birmingham, Alabama 35203

1710 Sixth Avenue North
Birmingham, Alabama 35203

105 Tallapoosa Street
Suite 200
Montgomery, Alabama 36104

30 Ivan Allen, Jr. Blvd., NW
Atlanta, GA 30308

1310 Twenty-Fifth Avenue
Gulfport, Mississippi 39501

401 East Capital Street
Suite 200
Jackson, Mississippi 39201

1275 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Disclaimer and Copyright

This publication is intended to provide general information. It is not intended as a solicitation, and in the event legal services are sought, no representation is made that the quality of legal services to be performed is greater than the quality of legal services performed by other lawyers. The listing of any area of practice does not indicate any certification of expertise in the area as listed. © 2008. Balch & Bingham LLP. All rights reserved.

IRS CIRCULAR 230
DISCLOSURE: Unless explicitly stated to the contrary, this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code.

it provides to open its accounts, the methods it provides to access its accounts and its previous experiences with identity theft.

When drafting an identity theft prevention program, banks should incorporate any Red Flags from specific incidents of identity theft that they have experienced and should also adopt the Red Flags that their regulators have identified as examples. These include:

- Address discrepancies.
- Photographs not matching customers.
- Inactive accounts.
- Notification of statements not being received.
- Downloading or accessing an unusually large number of customer account records.

A list of these Red Flags is attached in an Appendix to the regulations.

DETECTING RED FLAGS

The program must contain policies and procedures for detecting the Red Flags that the bank has identified. Detecting Red Flags can be accomplished through obtaining identifying information about a person opening an account and verifying their identity, authenticating customers, monitoring transactions and verifying the validity of change of address requests, in the case of existing accounts.

There are several tools that a bank can use to detect Red Flags. When opening an account, a Red Flag checklist can be very helpful. Some Red Flags are triggered by specific events and can be detected upon review of the account after such event has occurred. Other Red Flags may be detected as part of a scheduled review.

RESPONDING TO RED FLAGS

The program must provide for appropriate responses when a bank has determined that a detected Red Flag evidences a risk of identity theft. Appropriate responses to Red Flags may include contacting the customer, changing passwords on an account, declining to open a new account, notifying law enforcement, assigning a new account number to an account or closing an existing account altogether.

A Red Flag response list may be useful so that the bank will respond consistently when certain Red Flags are detected. Because responding to Red Flags can be very fact specific banks should consider all

circumstances that are relevant to the detected Red Flag and respond appropriately.

UPDATING THE PROGRAM

The identity theft prevention program should be updated periodically based on the experiences of the bank with identity theft, changes in the methods of identity theft, changes in the types of accounts offered and maintained by the bank and changes in the business structure of the bank. Updates to the program should include updates to the risk assessment, the identified Red Flags and the training of affected personnel.

ADMINISTRATION OF THE PROGRAM

Each bank that is required to implement a program must provide for the continued administration of the program and must:

- (1) Obtain approval of the initial written program from either its board of directors or an appropriate committee of the board of directors;
- (2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the program;
- (3) Train staff, as necessary, to effectively implement the program; and
- (4) Exercise appropriate and effective oversight of service provider arrangements.

CONCLUSION

Even before the deadline date of November 1, 2008, banks can expect that their federal banking examiners will want to see evidence that an identity theft prevention program is either in place or is under development. Management should be scheduling time during a board meeting in the next several months for the board or a board committee to approve a formal written program. If ongoing oversight of the program is to be handled by the board or a board committee, rather than by senior management, as discussed above, then board agendas and/or materials should also reflect that fact in future years.

Examiners will also expect that if a bank experiences an identity theft incident with one of its customers, prevention of future similar incidents is specifically reflected in its program.