Society of Corporate Compliance & Ethics

Compliance and Ethics Magazine

Volume Six
Number One
February 2009
Bimonthly

Meet

Ann Oglanian

Managing Director, ReGroup, LLC

PAGE 16

Earn CEU Credit

SEE PAGE 44

The Economy!

By Roy Snell, CEO, SCCE

PAGE 15

The Red Flag Provisions: Impact on creditors and facilitating compliance

page 52

SCCE is going green

SCCE conference attendees will NOT automatically receive conference binders. If you would like to purchase conference binders, please choose that option on your conference registration form. Attendees will receive electronic access to course materials prior to the conference as well as a CD onsite with all the conference materials.

Also:

Global Compliance: India

PAGE 28

The Red Flag Provisions: How technology can facilitate compliance

By Heather Czermak, Tom Leuchtner, and Steven Lefar

Editor's note: Heather Czermak is Senior Product Manager for Wolters Kluwer Financial Service. She can be reached at heather.czermak@wolterskluwer.com

Tom Leuchtner is Senior Product Manager for Fraud for Wolters Kluwer Financial Services. He can be reached at tom.leuchtner@wolterskluwer.com.

Steven Lefar is General Manager, MediRegs and Director, Healthcare for Wolters Kluwer Law and Business. He can be reached at steven.lefar@wolterskluwer.com

Overview

The Red Flags provisions of the Fair and Accurate Credit Transactions (FACT) Act took effect on Nov. 1, 2008, although the FTC announced it will suspend enforcement until May 2009. Despite the final regulations being issued October 31, 2007, there has been confusion as to how institutions can rapidly deploy an effective Red Flags rules program while regulators have issued little to no guidance on how to do so. The good news is that most institutions already have the processes and technology systems in place that can be leveraged in developing their Red Flags rules program. However, a dedicated effort needs to be employed to ensure appropriate compliance with the new requirements.

The Red Flags rules are applicable to many kinds of institutions and apply broadly to any "Creditor" handling "Covered Accounts:"

> A Creditor is any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. (15 U.S.C. §§ 1691a(e), 1681a(r)(5). 16 C.F.R. § 681.2(b)(4))

Creditors that offer or maintain covered accounts have obligations under the Red Flags regulations. A covered account is:

> (i) An account that a financial institution or creditor 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 that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. (16 C.F.R. § 681.2(b)(3))

Red Flags issues are not just for financial institutions. Any company that regularly extends or merely arranges for the extension of credit is also subject to the rules. In particular, creditors in the health care field may be at risk of medical identity theft (i.e., identity theft for the purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk. (72 Fed. Reg. 63727 (Nov. 9, 2007)). Health care providers create a credit relationship when they set up an account that may have a payment plan or consist of a multi-tier payment. For a detailed analysis of health care Red Flags rule issues as well as medical identity theft, the World Privacy Forum has done critical analyses of the topic; visit www.worldprivacyforum.org.

Regulatory Provisions

Red Flags provisions are intended to help consumers fight the growing crime of identity theft, which can entail stealing a credit card number, or impersonating someone to gain access to a credit account or medical or other benefits. Medical identity theft is particularly harmful, since it not only uses up the victims' benefits, it also creates the potential for life threatening issues if the wrong data is entered in a medical record. In an appendix to the requirements, regulators list 26 suggested "Red Flags" as indicators of possible identity theft. If a red flag is detected, it doesn't necessarily mean that identity theft has occurred; it means that the institution should investigate the warning and document an appropriate response. All institutions and other creditors with "covered accounts," including consumer loans and deposit accounts, need to comply.

The Red Flags rules are comprised of three regulations. These include requirements for an identity theft prevention program, address discrepancy require-

Examples of Red Flags Rules in Health Care (http://www.worldprivacyforum.org)	Example of Red Flags Rules in Banks
■ A complaint or question from a patient based on the patient's receipt of: ❑ bill for another individual ❑ bill for a product or service that the patient denies receiving ❑ bill from a health care provider that the patient never patronized ❑ notice of insurance benefits (or Explanation of Benefits) for health services never received. ■ Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient. ■ A complaint or question from a patient about the receipt of a collection notice from a bill collector. ■ A patient or insurance company report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached. ■ A complaint or question from a patient about information added to a credit report by a health care provider or insurer. ■ A dispute of a bill by a patient who claims to be the victim of any type of identity theft. ■ A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance. ■ A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.	■ ATM Transaction of Dormant Account ■ Deposits Increase Compared to Last 6 Months ■ New Credit Account Credit Limit Exploitation ■ New Request After Address Change ■ Transaction Increase Compared to Last 6 Months ■ Withdrawal Increase Compared to Last 6 Months

ments and requirements for card issuers. Each institution that holds any consumer account or other account for which there is a reasonably foreseeable risk of identity theft is required to develop and implement an Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts. The program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft and enable an institution that grants financial credit to:

- Identify relevant patterns, practices and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the program;
- Detect red flags that have been incorporated into the program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the program is updated periodically to reflect changes in risks from identity theft.

In addition to identity theft prevention, the institution is required to investigate address discrepancies. For institutions accessing consumer reports, they must implement reasonable policies and procedures to investigate notice of address discrepancy from a consumer reporting agency. Institutions are also required to identify a substantial difference between the address provided by the consumer and that reported in the agency's file for the consumer. In regards to card issuers, requests for change of address must be verified prior to issuing an additional or replacement card if the request is received within 30 days after notification. An additional or replacement card cannot be issued until you assess the validity of the change in address.

Red Flags Program

The single most important aspect of any institution's effort to create and implement a Red Flags program should be defining the program itself. The basic requirement mandated by the regulations is that a documented program exist and that it be approved by the board of directors. A key factor in constructing a successful written identity theft control program depends on making sure key business units and stakeholders are represented. Input from this cross-functional team will help to facilitate a complete risk assessment of the institution's covered accounts to determine relevant red flags.

To meet these regulatory requirements, technology can help facilitate a rapid program deployment including program

Continued on page 54

design, program documentation, customer identification, ongoing assessment, account monitoring and reporting.

Leveraging Automation

Many institutions are leveraging automation to detect the identified relevant red flags. In addition to providing real-time data validation against current data sets, automated solutions reinforce internal policies and procedures consistently throughout operations.

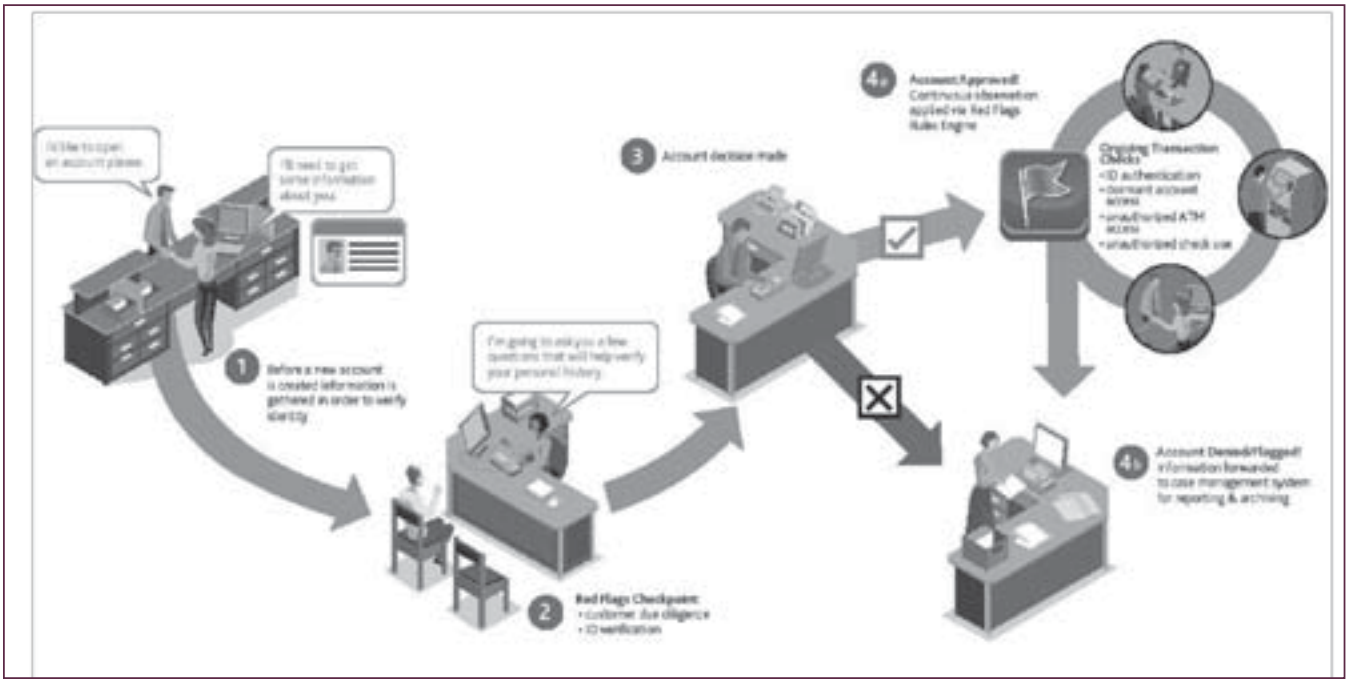
Many financial institutions have already implemented technology to facilitate identity verification and authentication for Bank Secrecy Act and anti-money laundering requirements. Through the use of comprehensive CIP software solutions, existing BSA/AML tests can be easily leveraged to meet Red Flags requirements for detection, investigation and reporting simultaneously. In the health care setting, identity verification for Medicaid, preauthorization of insurance and other techniques are often embedded into patient financial services processes. Existing Customer Identification Programs (CIP) and Customer Due Diligence (CDD) controls provide many of the required validations for new and existing customers.

In addition to identity theft red flags detection, ongoing monitoring of accounts and employee activity can be facilitated through automated solutions. These systems monitor all account and employee activity in real-time and provide automated alerts on ID theft activities, such as account beneficiary, address or name changes that may be of a suspicious nature. There are often common patterns of this kind of activity that our behavioral monitoring can detect, even though these patterns are often difficult to differentiate from normal business activities. Sometimes employing an automated system can generate "false positive" alerts, so systems need to manage that as well.

Finally, to help with sifting through the volumes of data and alerts and weed out false positives, a case management services platform can greatly enhance the tracking and management of ID theft cases while facilitating the productivity and workflow of reporting and filing. These systems facilitate the data collection of red flags detection information from the automated solutions (if properly integrated) while keeping case information organized and up-to-date. They also provide an enterprise view of cases for any type of fraudulent activity.

Technology solutions need to cover all three regulatory requirements: identity theft prevention, address discrepancy, and card issuer requirements for new and existing covered accounts. The guidelines for detecting red flags indicate that address detection for new and existing accounts should be accomplished by "Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules." So, the use of a CIP verification solution to detect identity theft red flags is a logical option.

Continued on page 56



Banking Example of Automated Solution

Because fraud scenarios are constantly evolving, it is important the red flags approach be flexible and extendable. As fraud schemes change, red flags rules must be enhanced to support the institution's policies and procedures. An integrated rules engine enables the institution to easily adjust existing rules and measures and add new requirements based on new fraud alerts. In addition, a configurable workflow helps to manage investigation, escalation and alerts in support of changing policies and procedures.

An institution can create management visibility to measure the effectiveness of the program by summarizing these efforts through ad-hoc and custom reporting.

These steps will help show an overview of the complete Red Flags program, detailing identification, detection, investigation and updating components, which is the ultimate goal.

Understanding the red flags and identify theft issues in your industry combined with intelligent automation can protect your customers and your organization. ■

Authors' note: WoltersKluwer has set up a Red Flag Resource Center to offer compliance information and software solutions to assist your organization. To view it, visit http://www.wolterskluwerfs.com/RedFlagAuthorRec.