

Identity Theft Red Flags Rule ... Are You in Compliance or Waving the White Flag?

BKD, LLP
Thomas W. Grundy, CRCM
Matthew A. Lathrom, CISM, CISA, MCP

Mitchell, Williams, Selig, Gates & Woodyard, PLLC
Todd L. Newton, Counsel

experience **BKD** MITCHELL WILLIAMS

Identity Theft Red Flags Rule – Call to Action

- Introductions
- Topics to be covered
 - ❖ Audience overview and survey question
 - ❖ Background of Rule
 - ❖ Primary components of Rule
 - ❖ Key definitions
 - ❖ Detection, prevention & mitigation of identity theft
 - ❖ Practical insights
 - ❖ Dealing with notice of address discrepancies

experience **BKD** MITCHELL WILLIAMS

Identity Theft Red Flags Rule – Call to Action

- Audience overview
 - ❖ Healthcare 56%
 - ❖ Education 28%
 - ❖ Other 16%
 - ✓ Government, Telecommunications, Financial Services, Insurance, Legal, and Not-for-profit Organizations
- Survey question
 - ❖ Where do you stand with your efforts to prepare for the Identity Theft Red Flags Rule?
 - ✓ Have a program built 11%
 - ✓ In process of building program 58%
 - ✓ Don't know about red flags 31%

experience **BKD** MITCHELL WILLIAMS

Identity Theft

- As many as nine million Americans have their identities stolen each year (FTC)
- Identity theft is single largest complaint category, representing 26 percent of all complaints received (FTC)
 - ❖ Identity theft complaints totaled 313,982 in 2008, up from 259,266 in 2007
- Approximately 250,000 medical identity theft cases were reported in 2006 (World Privacy Forum)
 - ❖ Electronic records, absent controls, accelerate pace of identity theft
 - ❖ Pollution of medical records is difficult to correct & can lead to improper medical diagnosis & treatment down the road

Identity Theft

- According to U.S. Department of Education, Office of Inspector General, college students are prime targets for identity theft
 - ❖ Almost half of all college students receive credit card applications on daily or weekly basis. Many of these students throw out card applications without destroying them
 - ❖ Nearly a third of students rarely, if ever, reconcile their credit card & checking account balances
 - ❖ Almost 50 percent of students have had grades posted by Social Security Number
 - ❖ 31 percent of identity theft victims fall into 18-29 age group

Identity Theft Red Flags Rule – Background

- Statutory/regulatory provisions
 - ❖ December 4, 2003 – *The Fair & Accurate Credit Transactions Act of 2003* (FACT Act) signed into law
 - ✓ Amended *Fair Credit Reporting Act* (FCRA)
 - ❖ November 9, 2007
 - ✓ Agencies published Final Rule effective November 1, 2008
 - ❖ October 22, 2008
 - ✓ FTC delayed enforcement of provisions requiring development of written identity theft prevention program until May 1, 2009, to give covered entities additional time to implement their program
 - ✓ **Note:** extension did not apply to requirements regarding notice of address discrepancies, thus "users" of consumer reports should already be in compliance.

Identity Theft Red Flags Rule – Background

- Two primary components of Red Flags Rule we will focus on
 - 1) Covered entities must implement written program to detect, prevent & mitigate identity theft in connection with “covered accounts.”
 - 2) “Users” of consumer reports must implement policies & procedures for dealing with receipt of notice of address discrepancy from consumer reporting agency.

Identity Theft Red Flags Rule – Covered Entities

- **Question:** “How does this apply to my organization?”
- **Answer:** Red Flags Rule has very broad definitions that cover variety of organizations based upon nature of their business & types of services they provide

Identity Theft Red Flags Rule – Key Definitions

- **“Creditor”**
 - ❖ Any person who regularly extends, renews, or continues credit
 - ❖ Any person who regularly arranges for extension, renewal or continuation of credit
 - ❖ Any assignee of original creditor who participates in decision to extend, renew or continue credit
 - ❖ **Note:** Rule specifically includes lenders, utility companies & telecommunications companies

Identity Theft Red Flags Rule – Key Definitions

- **“Account”**
 - ❖ Continuing relationship established by person with financial institution or creditor to obtain product or service for personal, family, household or business purposes

- **“Covered Account”**
 - ❖ Consumer account designed to permit multiple payments or transactions (credit card account, car loan, cell phone account, utility account, etc.)
 - ❖ Any other account for which there is reasonably foreseeable risk to customers or to safety & soundness of organization from identity theft

Identity Theft Red Flags Rule – Key Definitions

- **“Identity Theft”**
 - ❖ Fraud committed or attempted using identifying information of another person without authority

- **“Red Flag”**
 - ❖ Pattern, practice or specific activity that indicates possible existence of identity theft

Identity Theft Red Flags Rule – Key Definitions

Given these broad definitions, several different types of organizations fall within scope of Red Flags Rule, including

- ✓ Colleges & universities
- ✓ Not-for-profit organizations
- ✓ Healthcare providers
- ✓ Local government entities
- ✓ Utility & telecommunications companies

Detection, Prevention & Mitigation of Identity Theft

Detection, Prevention & Mitigation of Identity Theft -- Regulatory Requirements

- Periodic identification of covered accounts
 - ❖ Each creditor must periodically determine whether it offers or maintains "covered accounts"
 - ❖ As part of this determination, it must conduct a risk assessment to determine whether it offers or maintains "any other account ... for which there is a reasonably foreseeable risk to customer or to the safety & soundness of the ... creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."

Detection, Prevention & Mitigation of Identity Theft -- Regulatory Requirements

- Identity Theft Prevention Program
 - ❖ Establish written program/policy to address identity theft appropriate to size & complexity of creditor & nature & scope of its activities
 - ✓ **Note:** Leverage risk assessment findings & adjust for changes in risk profile

**Detection, Prevention & Mitigation of Identity Theft --
Regulatory Requirements**

- **Written identity theft program must include reasonable policies & procedures to:**
 - ❖ Identify relevant Red Flags for covered accounts, incorporating those Red Flags into program
 - ❖ Detect Red Flags that have been incorporated into program
 - ❖ Respond appropriately to any Red Flags that are detected to prevent & mitigate identity theft
 - ❖ Ensure program is updated periodically to reflect changes in risks to customers & to safety & soundness of creditor from identity theft

Note: Appendix A of Rule contains detailed guidelines for developing & implementing identity theft program.

**Detection, Prevention & Mitigation of Identity Theft --
Regulatory Requirements**

- **Administration of program**
 - ❖ Board or appropriate committee must approve written program
 - ❖ Involve board, appropriate committee of board, or designated employee at level of senior management in oversight, development, implementation & administration of program
 - ❖ Train staff to effectively implement program
 - ❖ Effective oversight of third party service providers

Practical Insights

Practical Insight Periodic Identification of Covered Accounts

Risk Assessment Process

Step 1: Identification of covered accounts

- ✓ Methods for opening accounts
- ✓ Methods to access accounts
- ✓ Review prior experiences with identity theft

Step 2: Map relevant Red Flags to covered accounts

- ✓ Establish appropriate responses to potential Red Flags

Step 3: Document controls to detect, prevent & mitigate identity theft

- ✓ Document escalation & response procedures when Red Flag is detected

Practical Insight Periodic Identification of Covered Accounts

Risk Assessment Process

Step 4: Identify gaps

- ✓ Action plans to remediate noted gaps & weaknesses

Step 5: Score the risks

- ✓ Impact of product or service from standpoint of volume & very nature of product or service
- ✓ Inherent risk of Identity theft occurring
- ✓ Residual risk considering controls in place

Step 6: Status all items with unacceptable score

- ✓ Assign ownership
- ✓ Establish date to resolve gap

Practical Insight – Example 1

- Hospital emergency room admission
 - ❖ Person shows up at emergency room seeking medical attention while using another person's identity
 - ✓ Legal implications
 - ✓ Risk management considerations
 - ✓ IT controls

Practical Insight – Example 2

- Application for utility account
 - ❖ Person applies for utility account using another person's social security number
 - ✓ Legal implications
 - ✓ Risk management considerations
 - ✓ IT controls

Practical Insight – Example 3

- Applying for a student loan
 - ❖ Person applies for a student loan using another person's social security number
 - ✓ Legal implications
 - ✓ Risk management considerations
 - ✓ IT controls

Notice of Address Discrepancies

Notice of Address Discrepancies – Key Definition

- “Notice of address discrepancy”
 - ❖ Notice sent to user of consumer report by consumer reporting agency that informs user of substantial difference between address for consumer that user provided to request consumer report & address(es) in agency’s file for consumer

Notice of Address Discrepancies

- Duties of users of consumer reports
 - ❖ Requirement to form reasonable belief
 - ✓ Must develop & implement policies & procedures designed to enable user to form reasonable belief that consumer report relates to consumer about whom it has requested report
 - ❖ Reasonable policies & procedures
 - ✓ Compare information in consumer report provided by consumer reporting agency with information user has on file or obtains from third-party sources
 - ✓ Verify information in consumer report provided by consumer reporting agency with consumer

Notice of Address Discrepancies

- Duties of users of consumer reports
 - ❖ Furnishing consumer’s confirmed address
 - ✓ User must have policies & procedures to furnish confirmed address for consumer to consumer reporting agency when user
 - Can form reasonable belief that report relates to consumer
 - Establishes continuing relationship with consumer
 - Regularly & in ordinary course of business furnishes information to consumer reporting agency

Other Key Considerations ...

- Regulatory examination, risk management & audit
 - ❖ Covered accounts
 - ❖ Training
 - ❖ Vendor management

- Penalties
 - ❖ Up to \$2,500 per violation for actions brought by FTC
 - ❖ Additional penalties including punitive damages for actions brought by states

Now What?

Reference

- Link to identity theft rules
 - ❖ [Identity Theft Red Flags & Address Discrepancies – Final Rule](http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf)
- <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>

Questions?

- Enter them using the GoToWebinar toolbar

Next BKD Webcast

- **Economic Conditions & Policy Response:
Implications for Business and Capital Markets**
 - ❖ Presented by BKD's Jeff Layman
 - ❖ Thursday, May 14
 - ❖ 10-11 a.m. Central time
 - ❖ Register now at www.bkd.com/webcast



Contact Information

Compliance/Audit: Thomas W. Grundy, CRCM
317.383.4191
tgrundy@bkd.com

Information Technology: Matthew A. Lathrom, CISM, CISA, MCP
816.701.0284
mlathrom@bkd.com

Legal: Todd L. Newton, Counsel
501.688.8881
newton@mwlaw.com


