



# Complying with the Red Flag Rules and Getting Ready for Data Breach Notification

---

Marc Zwillinger

[mzwillinger@sonnenschein.com](mailto:mzwillinger@sonnenschein.com)

(202) 408-9171

To participate in the audio portion of the  
webcast, please dial **800.954.1052**

# What are the Red Flag Rules?

---

- The Red Flag regulations require companies to develop and implement written identity theft prevention programs designed to detect, prevent, and mitigate identity theft.
- The regulations also cover instances where a creditor receives a notice of an address discrepancy from a consumer reporting service.
- They are not data security rules.
- Goal is to “ensure that your business is on the lookout for the signs that crook is using someone else’s information, typically to get products or services from you with no intention of paying.”

# Summary of Rule

---

- Create and implement a comprehensive written program designed to prevent, detect, and mitigate foreseeable risks of identity theft.
- 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.
- Ensure the Program is updated periodically to reflect changes in risks from identity theft.
- Provide oversight of service providers used by the company

# Who must comply?

---

- **“Creditors” offering “covered accounts”**
- **Who is a creditor?**
  - Any entity that regularly defers payment for goods or services or provides goods or services and bills customers later. Utility companies, health care providers, and telecommunication companies are specifically designed to be covered.
- **Financial institutions**
  - The term “financial institution” means a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account (as defined in section 461(b) of Title 12) belonging to a consumer. 16 C.F.R. 681.2(b)(7); 15 U.S.C. 1681a(t).

# Covered Accounts

---

- If you are a creditor – you must then examine whether you have covered accounts
- Covered accounts are those accounts that:
  - Are primarily for personal, family or household purposes that involves are is designed to permit multiple payments or transactions
  - Any other account (including business) for which there is a reasonably foreseeable risk to consumers or the safety and soundness of the creditor from identity theft.

# When must parties comply?

---

- All entities under the FTC's jurisdiction must be in compliance by **May 1, 2009 (extended from Nov. 1 2008)**:
  - A written plan must be approved by the board or an appropriate subcommittee.
  - Provide training to employees and service providers that may access covered accounts.
  - The board, a subcommittee, or a **member of senior management** must monitor the development, implementation, and administration of the program, receive annual reports on effectiveness, and approve any material changes.

# How do providers comply?

---

- Process for implementation:
  - **Identify** relevant red flags and perform an identity theft risk assessment.
  - **Review** the appendix to the red flag rules and specifically consider those red flags.
  - Create a list of **triggers** that, when present, will cause the company to take action and develop methods to **detect** those triggers in connection with new and existing accounts
  - Provide a process for **escalation** to respond to any triggers detected.

# Step One: Identify

---

- The rules require covered entities to “[i]dentify relevant Red Flags for the covered accounts that the ... creditor offers or maintains, and incorporate those Red Flags into its Program.”  
16 C.F.R. § 681.2(d)(2).

# Step One: Identify

---

- What are Red Flags?
  - Red Flags are those events that the FTC says should alert an organization that there is risk of identity theft
- Drawn from:
  - The entity's own history of Identity Theft
  - The FTC's suggested list of red flags

# **Step One: Identify based on Risk Assessment and Prior Experience**

- Assess the risk factors for identity theft
  - Types of covered accounts
  - Methods for opening new accounts
  - Methods for accessing existing accounts
- A review of prior experiences with identity theft
- A defined goal
  - Plan should include detection and escalation procedures that allow the health care provider to respond before identity theft occurs.

# Step Two: Review Appendix

---

- The appendix to the Red Flag rules provides 5 categories of Red Flags to consider:
  - Alerts, Notifications or Warnings from a Consumer Reporting Agency
  - Suspicious Documents
    - Forged ID, falsified health insurance cards.
  - Suspicious Personal Identifying Information
    - Info is inconsistent with other personal information provided by the patient. For instance, a lack of correlation between SSN and DOB.
  - Unusual or Suspicious Account Activity
    - Nonpayment when there is no history of late payment, material change in spending patterns.
  - Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

# Step Three: Identifying and Detecting Triggers

---

- After reviewing its own experience and the Appendix, health care providers must create a list of “triggers” or Red Flags that they will attempt to detect and when detected, take action to prevent identity theft. 16 C.F.R. § 681.2(d)(2)(ii).
- Detection methods must include means:
  - For “obtaining information about and verifying the identity of a person opening an account” and
  - “Authenticating customers, monitoring transactions, and verifying the validity of change of address requests.”
  - Often based on electronic data, reports generated, etc.

# Step Four: Escalation

---

- A plan to “respond appropriately to any Red Flags that are detected.” 16 C.F.R. § 681.2(d)(2)(iii).
- A process to escalate detected triggers to employees that can take action to prevent or limit identity theft.
- *E.g.* what you do when you detect a trigger.

# Escalation

---

- Monitor accounts
- Contact customer based on information on file
- Refuse to provide credit (where permissible by law)
- Not attempting to collect on a covered account or not selling a covered account to a debt collector may also be a proper response.
- Notify law enforcement
- “No response” can be a proper response to a Red Flag.

# Example

---

- Risk assessment – in the past we provided service to a patient pretending to be someone else 15 times, which we later discovered.
- Identify Red Flag – Suspicious Documents (Forged Health Insurance Card)
- Create trigger – when patient comes in, we will always ask to see Health Insurance card – if the document looks improper we will: ask to see photo identification
- If suspicious or no ID, we will escalate issue to Supervisor of Patient Services for investigation
- Supervisor of Patient Services will investigate and determine ID of patient and ID of person we are billing and their relationship

# Implementation

---

- The final plan must be presented to the Board of Directors, or a subcommittee, for approval. 16 C.F.R. § 681.2(e)(1).
- The health care provider must then train staff and put in place methods for supervising any service providers that may access covered customer accounts — such as billing or collection agencies. 16 C.F.R. § 681.2(e)(3) & (4).
  - Providers need not retrain personnel already trained for fraud.
- This training, education and monitoring feature may be folded into the health care provider's existing, broader corporate compliance program related to its health care and other activities.
- The Board must continue to exercise oversight over the development, implementation, and administration of the program. 16 C.F.R. § 681.2(e)(2).

# Reporting

---

- A covered entity must report on at least an annual basis regarding the identified incidents and effectiveness of the Program.
- Those reports should address compliance with the plan, significant identify theft incidents, and recommendations for material changes in the Program.

# Changing the Program

---

- Any material changes made because of new information must be approved by the Board of Directors or senior management. 16 C.F.R. § 681.2(e)(2).
- Changes to the Program may be warranted based on:
  - New experiences with identify theft;
  - Changes in identity theft methods;
  - Changes in the methods to detect, prevent and mitigate identity theft;
  - Changes in the types of accounts offered; and
  - New mergers, acquisitions, or alliances involving the health care provider.

# Address Discrepancy Rules

---

- Only applicable if a provider is a “user” of consumer reports.
- Triggered when a user receives a notice of address discrepancy from a consumer reporting agency pursuant to 15 U.S.C. § 1681c(h)(1).

# Address Discrepancy Rules

---

- Users must have procedures in place to enable them to form a reasonable belief that a consumer report relates to the consumer for whom the report was requested.
- Achieved by comparing consumer provided information with information:
  - Used to verify identity
  - In the user's own records
  - From third-party sources, or
- Verifying the information in the consumer report with the consumer.

# Address Discrepancy Rules

---

- Users must also have procedures to determine that the address it has furnished to the consumer reporting agency is accurate.
- Users may confirm address accuracy by:
  - Verifying the address with the consumer about whom it has requested the report
  - Reviewing its own records to verify the address of the consumer
  - Verify the address through third party sources
  - Using other reasonable means

# Address Discrepancy Rules

---

- The policies and procedures developed to comply with these rules must provide that the user will furnish the address the consumer has confirmed is accurate to the consumer reporting agency.

# Potential Liability for Non Compliance

---

- Administrative Enforcement: FCRA provides the FTC with a mechanism for enforcing the statute and its regulations. 15 U.S.C. § 1681s(a)(1). The FTC may seek a civil penalty of not more than \$2,500 per violation. 15 U.S.C. § 1681s(a)(2)(A).
- State Enforcement: A State may bring an action to enjoin a violation and seek damages on behalf of its residents seeking statutory damages of not more than \$1,000 per violation.
- Civil Liability: There is no private right of action for violations of the Red Flag rules. But there is a private right of action for violations of the address discrepancy rules.

# Health Information Technology for Economic and Clinical Health Act

---

- HITECH Act:
  - Extends the reach of HIPAA Privacy and Security Rules
  - Imposes Data Breach notification requirements for HIPAA-covered entities and business associates
  - Increases individuals' rights with respect to Protected Health Information ("PHI")
  - Increases enforcement of, and penalties for, inadequate protection of privacy and security of PHI

# Breach Notification Provisions in the HITECH Act

---

- Before the amended CA breach statute took effect on 01/01/09, only Arkansas included medical information in the definition of “personal information” triggering breach notification obligations;
- Breaches of medical information that did not involve financial information often went unreported.
- 2008 – California amended statute to include both “medical information” and “health insurance information”
- HITECH Act imposes breach notification requirements on all HIPAA-covered entities and business associates.
- Effective date – HHS required to issue interim final regulations NLT 180 days after enactment (August 17, 2009), which will become effective 30 days after publication (Sept. 17, 2009).

# Breach of unsecured PHI:

---

- Unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of PHI, except in situations when an unauthorized person to whom the information is disclosed “would not reasonably have been able to retain such information.”
- **\*\*Applies to both electronic and hard copy information.\*\***

# Notice

---

- Notice must be provided “without unreasonable delay” and no later than 60 days after breach is discovered;
- Via first-class mail unless the individual has specified a preference for email;
- Media notice – if PHI of more than 500 individuals in one state is breached, the entity must notify “prominent media outlets” in the state;
- HHS notice – covered entities must notify HHS of the breach:
  - More than 500 affected individuals – must notify HHS immediately
  - Less than 500 affected individuals – may notify HHS via an annual log of events.
- Business associates must notify the covered entity of the breach;

# Content of Notice:

---

- Description of facts about breach;
- Type of PHI involved;
- Steps individuals should take to protect themselves;
- What the covered entity is doing to investigate the situation and prevent future breaches; and
- Contact information for individuals to ask questions.

# What to do now?

---

- Sit and wait. .. Or, better yet
- Adopt Incident Response policy with breach notification
- Establish procedures and incident response team to respond to breach
- Identify systems that have covered data
- Assign internal roles and responsibilities, identify external vendors
- Consider incident response insurance policies

# DISCLAIMER

---

- These materials should not be considered as, or as a substitute for, legal advice and they are not intended to nor do they create an attorney-client relationship. Because the materials included here are general, they may not apply to your individual legal or factual circumstances. You should not take (or refrain from taking) any action based on the information you obtain from these materials without first obtaining professional counsel. The views expressed do not necessarily reflect those of the firm, its lawyers, or clients.

Sonnenschein  
SONNENSCHHEIN NATH & ROSENTHAL LLP