PIVOTGROUP
Armed with Information Security Knowledge

Red Flag Rules: What Do They Mean to Your Financial Institution?

by Faith M. Heikkila, Pivot Group Regional Security Services Manager – Great Lakes

Personally identifiable information (PII) is typically defined as a combination of first name or first letter of first name with last name and any of the following: Social Security Number (SSN), driver's license number, telephone number, address, credit or debit card number, bank account number, personal identification number (PIN), password, or username with password. If bank records are compromised by unauthorized access, which could include the unauthorized access by an employee without appropriate permission rights to access files containing PII, a security breach incident has occurred. Adequate notification is necessary after the determination has been made that this data is in fact, in the wild. Typically, consultation with an expert or attorney is necessary to determine if the PII has been inappropriately exposed to unauthorized persons. In the event that an employee without the correct credentials accesses the information, it must be verified whether or not they have released any details from such access into the public domain in order to determine if notice to affected customers is required.

FFIEC and FDIC Guidelines for Financial Institutions

Financial institutions want the confidentiality, integrity, availability, and non-repudiation of customer information protected. The Federal Financial Institutions Examination Council (FFIEC) issued guidelines for safeguarding high risk transactions, such as online money transfers in 2005 with the expectation that financial institutions would comply by January 1, 2007. Security breach incidents received more press in 2007 as more and more security breach incidents made national news headlines. As a result, FFIEC regulators have become more concerned with the integrity of online banking systems.

The FFIEC guidelines mandate that financial institutions develop an appropriate security program by utilizing a risk assessment, followed by the use of authentication appropriate for the level of risk. The FFIEC states that single-factor authentication is clearly an unacceptable control mechanism for high risk transactions involving personally identifiable customer information. Hence, it is suggested that multi-factor authentication, multi-layered (defense-in-depth) security, and other controls reasonable to mitigate risk be implemented. Additionally, the FDIC (Federal Deposit Insurance Corporation) and FFIEC (Federal Financial Institutions Examination Council) have supplemented red flag regulations to its guidelines.

Red Flag Rules

As a result of the propagating identity theft market, wherein the stakes have been raised by organized crime entering the playing field, the FDIC drafted a supervisory policy on identity theft that was issued on April 11, 2007. On October 31, 2007, the Federal Trade Commission, FFIEC, FDIC, and NCUA (National Credit Union Administration) sent the *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003* to the *Federal Register* for publication of the final rule. These red flag rules have a mandatory compliance date of **November 1, 2008** by all financial institutions.

The red flag rules require financial institutions to implement a written identity theft prevention program and take specific steps to prevent identity theft. The financial institution must track events to develop patterns of identity theft as an early warning system to proactively notify their customers and the appropriate authorities. Examples of specific events that financial institution should monitor as possible indicators of identity theft are suspicious or unusual account activity that is inconsistent with previous account activity, consumer fraud alert received from a consumer reporting agency, suspicious identification documents that appear to be altered or forged, and suspicious access to PII.

As the **November 1, 2008 deadline** approaches, financial institutions are looking for assistance with their risk assessments in order to substantiate whether or not they have developed a program sufficient to address the Identity Theft Red Flag Rules outlined in the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003. According to these rules, financial institutions must develop a Red Flag Program to address inconsistencies detected in the activities, identification of customers, and practices of its customers.

look, **plan**, **act**, **repeat**

- **look** – Risk Assessment of Your Red Flag Program
  - Identify procedures and policies to follow with regard to:
    - How red flags will be identified, implemented, and recorded
    - The incident response plans for mitigating and identifying ID theft

- **plan** – Build a Proactive Red Flag Strategy
  - Set up a framework with the approval of the board of directors or an oversight committee
  - Identify how to mitigate ID theft risks
    - Technical controls
    - Management controls
    - Operational controls
  - Draft or revise security policies to cover these risks
  - Select potential technologies
  - Education program for employees and customers

- **act** – Take Action on the Red Flag Strategy Plan
  - Implement the processes, controls, and technologies
  - Revise security policies as required
  - Train customers and employees on security best practices

- **repeat** – The Life Cycle of the Red Flag Program is a Process Not a Destination
  - Periodic analysis of what worked and what procedures need to be updated as ID theft attempts change
  - Ongoing basis – repeat it on a regular basis as security best practices indicate
  - Schedule regular risk assessments and update policies/controls regularly
  - If new technology is employed, schedule a risk assessment
  - If business requirements change, schedule a risk assessment

Faith M. Heikkila *is Pivot Group's Regional Security Services Manager for the Great Lakes and has more than 18 years of paralegal and IT project management experience. She's currently a PhD candidate in information systems specializing in information assurance at Nova Southeastern University. Her research interests include secure remote access to organization databases, information security policies/procedures, and privacy issues. She is a member of the Michigan InfraGard Executive Board, the West Michigan InfraGard Advisory Panel, and the ConnecTech Greater Kalamazoo Board. She is a member of the ACM, the Association of Information Technology Professionals (AITP), the Computer Security Institute (CSI), the IEEE, and the Information Systems Security Association (ISSA). Review Faith's other publications at: http://pivotgroup.net/whitepapers.html or she can be reached at fheikkila@pivotgroup.net.*