Identity Theft Prevention Program

Implemented January 1, 2009
Updated: July 20, 2009
Updated: December 18, 2009

I. PROGRAM ADOPTION

The City of West Linn ("Utility") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed with oversight and authorization of the City Manager. After consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities, the City Manager determined that this Program was appropriate for the City of West Linn, and therefore approved this Program on January 1, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

2. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

"Identifying information" is defined under the Rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the Utility considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The Utility identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings From Credit Reporting Agencies

Red Flags

1) Report of fraud accompanying a credit report;
2) Notice or report from a credit agency of a credit freeze on a customer or applicant;
3) Notice or report from a credit agency of an active duty alert for an applicant; and
4) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Breach in the Utility's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the Utility from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS.

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, Utility personnel will take the following steps to monitor transactions with an account:

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;

6. Reopen an account with a new number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information

In order to further prevent the likelihood of Identity Theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for utility purposes.

VI. PROGRAM UPDATES

The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. In doing so, the Program Administrator will consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the Utility's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present to the City Manager his or her recommended changes and the City Manager will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Program Administrator who may be the head of the Utility, head of Finance, or his or her

appointee. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Utility staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Utility staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. *(The Utility may include in its Program how often training is to occur. The Program may also require staff to provide reports to the Program Administrator on incidents of Identity Theft, the Utility's compliance with the Program and the effectiveness of the Program.)*

C. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the Utility's Program and report any Red Flags to the Program Administrator.

D. Non-disclosure of Specific Practices

(This provision is not required by the Rule, but municipal utilities may find it useful.)

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices must be limited to the Identity Theft Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered “security information” as defined in Minnesota Statutes Section 13.37 and are unavailable to the public because disclosure of them would be likely to substantially jeopardized the security of information against improper use, that use being to circumvent the Utility’s Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.

Attachments

Identifying Information

PowerPoint explaining Identity Theft Red Flag Rules

IDENTIFYING INFORMATION

Identity Theft and Red Flags Rule requirements

The Red Flags Rule implements portions of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Section 111 of FACTA defines "Identity Theft" as "fraud committed using the identifying information of another person."

Under the Red Flags Rule, every financial institution and "creditor" (defined below) is required to establish an Identity Theft Prevention Program tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

- Identify relevant Red Flags for new and existing "covered accounts" (defined below) 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 to customers or to the safety and soundness of the creditor from Identity Theft.

The Rule requires the Program to be approved by "a designated employee at the level of senior management."

Definitions related to municipal utilities

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. Accounts maintained by a municipal utility that are covered by the Rule are all the individual utility service accounts held by customers of the utility whether residential, commercial or industrial.

The Rule defines creditors to "include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

Under the Rule, a "covered account" is:

- Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
- Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

"Identifying information" is defined under the Rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." It specifically includes all of the items listed below.

- Name
- Address
- Telephone number
- Social security number
- Date of birth
- Government issued driver's license or identification number
- Alien registration number
- Government passport number
- Employer or taxpayer identification number
- Unique electronic identification number
- Computer's Internet Protocol address
- Routing code

The tables on the following two pages are intended as tools to assist your Identity Theft Prevention Committee in identifying specific Red Flags and procedures at your utility for incorporation into your utility employee training and, as desired, your written Identity Theft Prevention Program. The items in each table may be used to generate discussion about Identity Theft threats and prevention and ought to be modified, expanded or refined as necessary.

"IDENTITY THEFT" (FRAUD) TYPE 1 – NEW ACCOUNTS

❒ Establishing utility service using another person's identity

Why would someone do it?

- The perpetrator defaulted on a past utility account or other account and so would not be eligible for service under his or her own name.
- The perpetrator intends to establish fraudulent proof of residency in order to commit fraud elsewhere.

Red flag:	**Detect whether fraud is being attempted or committed:**	**Prevent or mitigate detected fraud:**
ID picture doesn't match person	Request additional ID	Do not open account
ID information doesn't match person	Request additional ID	Do not open account
ID does not look authentic	Request additional ID	Do not open account
ID looks doctored	Request additional ID	Do not open account
Using a suspicious name	Request additional ID	Do not open account
Applicant requests that bill be sent to address different from where service is received	Verify that customer is connected to billing address (But be aware of the state's "Safe at Home" program)	Do not open account
Account for a residential address established under business name (to avoid using own bad name)	Obtain credit report on the individual	Do not open account
Credit report contains fraud warning, credit freeze notice or active duty alert	This may be an automatic fraud detection Red Flag	Notify Program Administrator; If warranted, notify law enforcement
Bill payment made under name other than that on utility account	Request proof of residence (other bills, etc.)	Close account

"IDENTITY THEFT" (FRAUD) TYPE 2 – EXISTING ACCOUNTS

❒ Continuing utility service under a another customer's name after he or she moves out

Why would someone do it?

- The perpetrator wants to avoid paying for service.
- The perpetrator defaulted on a past utility account or other account and so would not be eligible for service under his or her own name.

Red flag:	**Detect whether fraud is being committed:**	**Mitigate detected fraud:**
Non-payment of previously current account	Call customer phone number on file	Discontinue service; close account
Utility service utilized after known move-out with no change of customer notice received by utility	Call customer phone number on file	Discontinue service; close account
Bill payment made under a name other than name on utility account	Call customer phone number on file	Discontinue service; close account

technolytics

Security Update on *Red Flag* Compliance

By Kevin G. Coleman
Strategic Management Consultant

Background

- **These agencies have jointly issued final rules and guidelines. Compliance deadline November 1, 2008.**
  - **Federal Trade Commission**
  - **National Credit Union Administration**
  - **Department of The Treasury**
  - **Federal Deposit Insurance Corporation**
  - **Federal Reserve System**
  - **Treasury Office of Thrift Supervision**
  - **Treasury Comptroller of Currency**
  - **When does the law take effect?**

Red Flag

Compliance

- **FACTA was passed in 2003. The final regulations were put into place in November of 2007. Full compliance is required by November 2008.**
  - **What is the cost of non-compliance?**
    - **FACTA specifically calls for civil penalties and fines. The act also allows for class action law suits.**

technolytics

It is in the news all the time!

Where Victims Go for Help

- FTC – 3%
- Other Federal Agency – 5%
- State Dept of Motor Vehicle Admin – 7%
- State AG or State Consumer Agency – 8%
- Lawyer – 12%
- Credit Bureau – 22%
- Local Police – 26%
- Credit Grantor – 43%
- Did Not Contact Anyone – 38%

Statistics

- Every 12 seconds 3.4 identities are stolen in the United States.
- Well over 250 million sensitive records have been lost or stolen from data bases across the country since January 2005. One out of every 2 Americans are in them.
- One out of every five Americans will have their identities stolen this year.
- If this crime continues to grow at its current rate, in the next five years virtually every American will have their Identity compromised in some way!
- Statistically 20% of your customers and employees will become a victim.
- Cost to design, implement, manage and update the required program is estimated at $0.32 up to $1.03 per identity.
  (Number of identities = customers + employees + contract workers + vendors)

Statistics

- According to a February 2008 Javelin Identity Fraud Survey Report, $45 billion was lost to identity thieves in 2007.
- Identity theft has been used by Al Qaeda to fund terrorist acts.
- 61% of Identity Theft reports to the FTC indicate the report was also NOT given to local law enforcement

Definitions

- **Under these rules a “creditor” is**
  - Any organization that regularly extends, renews, or continues credit
  - Any organization that regularly arranges for the extension, renewal, or continuation of credit.
  - Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

- **A “covered account” is**
  - A consumer account designed to permit multiple payments or transactions
  - Any other account for which there is a reasonably foreseeable risk from identity theft.

- **A “transaction account is**
  - a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

Definitions

- A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. 681.2(b)(9)
- Identity Theft is a fraud committed or attempted using the identifying information of another person without authority.
  - Every state now has statutes covering identity theft.
  - Thirty-eight states have enacted data breach notification laws that are tightly coupled to identity theft.

Red Flag

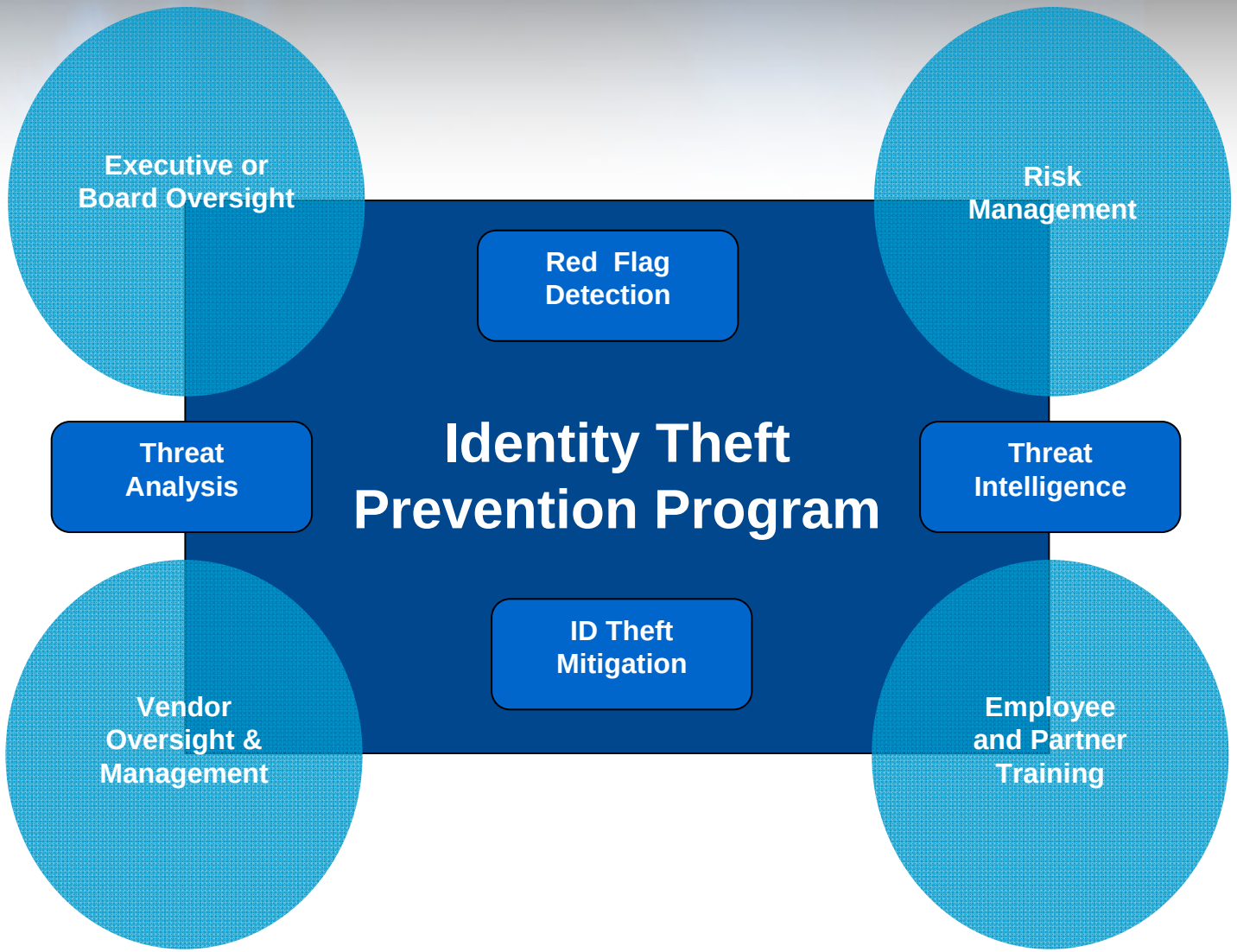
Compliance

October 2008 - "President Bush signed into law a bill that seeks to make it easier for prosecutors to go after cyber crooks, while ensuring that identity theft victims are compensated for their time and trouble when convicted identity thieves are forced to cough up ill-gotten gains."

You're required to comply if you are...

- Automotive dealers / Leasing organizations
- Banks/Credit unions/ payroll advances
- Debt collection agencies
- Credit / finance companies
- Financial institute & Insurance companies
- Mortgage brokers / Real Estate Brokers
- Colleges / Universities / Trade Schools
- Retailers who extend credit to consumers
- Telecommunications / Utility companies
- Any company that allows customers to buy on credit
  - Dental and medical service provider
  - Healthcare companies
  - Insurance broker
  - Legal service provider

The Program


Executive or Board Oversight
Risk Management
Red Flag Detection
Threat Analysis
Identity Theft Prevention Program
Threat Intelligence
ID Theft Mitigation
Vendor Oversight & Management
Employee and Partner Training

Red Flag Requires

- A written Information Security Policy and an Acceptable Use Policy.
- Data Handling Policy. Controls to prevent and mitigate the risks associated with identity theft.
- Program must be administered by a board of directors or a member of senior management.
- A compliance report must be delivered on at least an annual basis.
- Programs must be updated periodically.
- Programs must contain an incident response plan.
- The program must ensure that vendors and suppliers are also compliant.

Non-Compliance Penalties

- Penalties & Fines
- Actual damages and/or $1,000 per victim and up to $2,500 for every transaction that occurred during non-compliance periods.
- Board and/or Senior Management is ultimately responsible for implementation, administration and periodic review of the program.

- Other implications include:
  - Brand Damage
  - Loss of Customers
  - Litigation Costs (defense)
    - Non-compliance exposes organizations to claims of negligence if identities are stolen.

Healthcare Specific

- Medical identity theft is a real concern in the health care sector and is included expressly in the Red Flag Rules Guidelines. The possibility of medical identity theft gives rise to a duty to monitor for the potential that patients may be victims, among other duties outlined by the new regulations.

- Hospitals and other health care providers that are "creditors" and maintain "covered accounts" must comply with the Red Flag Rules by implementing a ***written*** identity theft prevention program. This written identity theft prevention program must be approved and adopted by the Board of Directors or equivalent governing body.

"The Red Flag Rules are an important opportunity for the health care sector to protect consumers and patients from the impacts of medical identity theft," said World Privacy Forum executive director Pam Dixon. "If implemented correctly, the new regulations could ease some of the problems consumers have been experiencing with the impacts of this crime."

Program Rules

- **Identify** "red flags" including relevant patterns, practices and/or activities that potentially implicate identity theft.
- **Detect** the "red flags" that are identified in the program.
- **Respond** to "red flag" incidents that are detected in order to prevent and mitigate the effects of identity theft.
- **Ensure** that the program is reviewed and updated periodically in order to adjust to changing and developing identity theft risks.

Red Flag

Compliance

Program Requirements

Red Flag program compliance requirements fall into five categories

1. alerts, notifications, or warnings from a consumer reporting agency
2. suspicious documents
3. suspicious personally identifying information, such as a suspicious address
4. unusual use of – or suspicious activity relating to – a covered account
5. notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

Program Administration

- Obtaining approval of the initial program by the board or a committee thereof
- Ensuring proper oversight of the program
- Training appropriate staff and vendors
- Oversee service provider arrangements

Red Flag

Compliance

Third Party Oversight

- Minimally, it means having a Red Flag security briefing with your service providers.
  - Clarify policies and procedures for handling consumer data, such as:
    - What detection mechanisms does the provider have?
    - How will you be informed when a red flag is detected?
    - How will you coordinate, if necessary, to respond to a red flag?

Red Flag

Compliance

Red Flag Officer

- The owner of the business or chief executive appoints or becomes the default Red Flag compliance officer. From this position red flags are processed red flags are strong warnings; but, remember most red flags will be quickly resolved. Your dealership identity theft detection program will:
  - be based on your current business practices
  - require a closer examination of all documents
  - require training of staff and possibly vendors
  - require a written report of the examination
  - require a written report for each red flag detected
  - require document access to be restricted
  - require documentation of disposal procedure

Red Flag

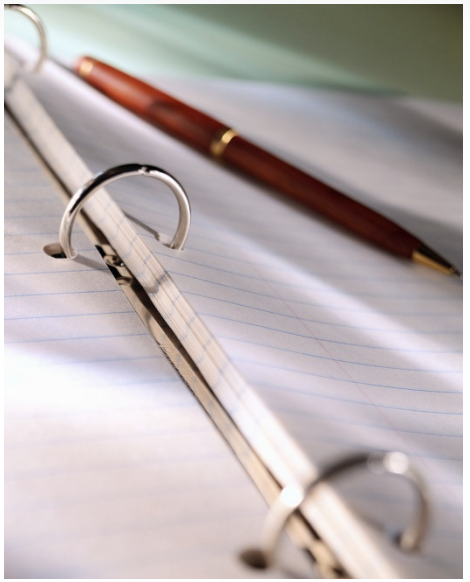
Compliance

Educate Potential Victims

- Educate potential victims about what to do If they are a victim of identity fheft.
  - Call the fraud departments of the three national credit agencies and ask them to put a fraud alert on your credit record. If your state allows it, ask them to “lock” your credit record from access.
  - If any fraudulent charge accounts have been opened (or taken over), notify the fraud department both by telephone and in writing.
  - Close all tampered or fraudulent accounts.
  - File a police report.
  - If the theft occurred out of town, notify that city’s police department.
  - Get copies of all police reports you file.

Red Flag Health Check

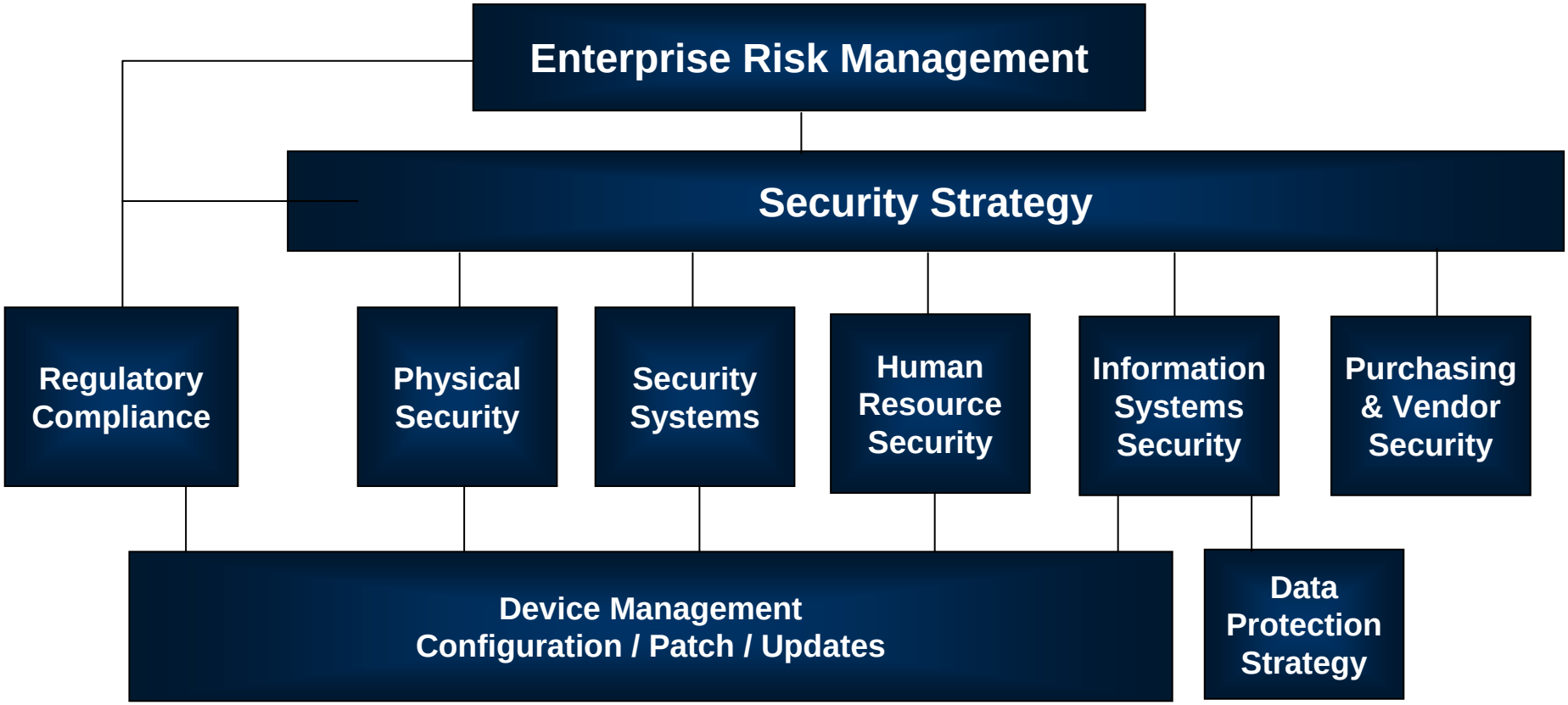
- Review and comment on the following.
  - Guide to privacy policy & procedure development
  - Incident response planning guide
    - Process
    - Reporting Form
    - Data Breach Law Matrix
  - Information Security Policy
  - Acceptable Use Policy
  - Annual Compliance Report
  - Sample Incident Response Plan
  - Data Handling Policy
  - Vendor Integrity Screening
  - Hiring and Termination Guidelines
    - Check List Hiring and Termination



Security Program Management

Strategy Requirements

Security professionals understand the link between improving security controls and Enterprise Risk Management. In order to reduce the overall risk for an organization, an integrated security strategy must be developed and implemented.



Security Solutionary with Solutionary

Whether you are implementing security management from scratch or improving an existing capabilities, it is necessary to consider and plan actions over both the short- and long-term. This is the heart of a security strategy.

Short-term (tactical) activities can achieve improvement in certain narrow areas and, most importantly, can generate the impetus and information to address broader and deeper-seated security problems. However, failure to address the long-term root causes of overall security is one of the most widespread and serious management issues today.

Technolytics partners with Solutionary for the delivery of exceptional security program development.

Identity Theft Contacts

- Contact the Identity Theft Resource Center at:
  - 858-693-7935
- Contact Federal Trade Commission at:
  - 800-IDTHEFT
- Contact Fraud Units of Credit Reporting Bureaus at:
  - EQUIFAX: 800-525-6285
  - EXPERIAN: 888-397-3742
  - TRANS UNION: 800-680-7289
- For fraudulent use of checks, contact:
  - Checkwrite: 800-766-2748
  - Chexsystems: 800-428-9623
  - Equifax Telecredit: 800-437-5120
  - National Processing Co.: 800-526-5380
  - SCAN: 800-262-7771

Other contacts

- Social Security Administration – 800-269-0271
- U.S. Postal Inspectors, if USPS involved – 800-275-8777
- State Department, if passport involved
- If checks missing or involved
  - TeleCheck – 800-710-9898
  - Certegy, Inc. – 800-437-5120
  - International Check Services – 800-631-9656

- FTC Identity Theft Hotline – 877-IDTHEFT (438-4338)

Solutionary Can Help

Solutionary specializes in delivering cost-effective, metrics-based information security and compliance services. As a pure-play MSSP, our focus on managed, monitored, compliance and advisory services helps clients mitigate risk, align with business objectives, and comply with standardized requirements.

www.solutionary.com info@solutionary.com 866.333.2133