Identity Protection Act

Training to Prevent Identity Theft

1

Identity Theft

- Identity Theft is the fastest growing crime in America.
- The Social Security number is a major privacy concern for most people, because it links to information that is typically kept private. Exposing and openly using SSNs has contributed to a growth in identity theft and other forms of credit card fraud. [1]

See References, Slide 17

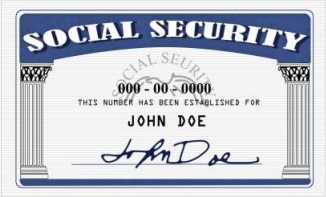
2

5 ILCS 179 Identity Protection Act

• Entered into effect June 1st, 2010.

•"The act prohibits certain uses of Social Security Numbers at public institutions and agencies, creates collection and protection requirements, and also requires state agencies to enact an identity protection policy for public view and for employees working with Social Security Numbers."

•Training is required of all employees of State Agencies that have access to Social Security Numbers (SSN).[2]



See References, Slide 17

3

Prohibited Activities

"A person or state or local government agency may not do the following:

1. Post or display an individual's SSN

2. Print an individual's SSN on any card that is used to retrieve any goods

3. Request an individual to provide his or her SSN on the internet, unless a secure connection is promised or the SSN is encrypted." [2]

See References, Slide 17

4

Prohibited Activities Cont.

4. Send an individual's SSN on any materials mailed or emailed to the individual unless:

- a. "State or federal law require the SSN to be mailed on the document.
- b. The document is part of the application or employment process and the SSN is included to establish, alter or terminate an account, or to validate the accuracy of that SSN.
- c. The SSN is not visible without opening the envelope."[2]

See References, Slide 17

5

Prohibited Activities Cont.

5. "Ask an individual to provide his or her SSN for entrance to a website

6. Use the SSN for a different purpose than it was collected for."[2]

See References, Slide 17

6

Exclusions for Sending or Storing Social Security Information

- If SSI is sent via email, it should be encrypted and it should contain a password.
- SSI may be mailed First Class or by UPS/FedEx.
- SSI should only be faxed when the person receiving it is readily available and it is sent to a place where no one else can receive it.
- SSI should only be stored on a flash drive that is district provided and secured.

See References, Slide 17

7

Exclusions For Collection of Social Security Numbers

- "SSNs may be revealed to employees, agents, contractors, or subcontractors of a government entity. The recipient of the information must give the original government entity a copy of their policy that explains how they abide by the Identity Protection Act.
- SSNs may be revealed to fulfill a court order, warrant, or subpoena.
- SSNs may be collected, used or disclosed for internal verification or other business purposes.
- SSNs may be collected and disclosed to ensure safety of state and local government employees.
- SSNs may be collected, used, or disclosed to locate a missing person, a lost relative or person who is due a benefit."[2]

See References, Slide 17

8

Public Inspection and Copying Requirement

- If a district collects SSNs and uses them on papers that could be publicly displayed, then the district must edit the SSNs before the examination or copying takes place.[2]

See References, Slide 17

9

Section 35 Identity Protection Policy

- The policy must include all of the following:

1. "Identify the Identity Protection Act.

2. Require all employees with access to SSNs to be trained to protect SSNs. Training should provide how to handle documents that contain SSNs from the collection time to the disposal time.

3. Confirm that only employees who can use or handle documents with SSNs have access to that information

4. Require that SSNs requested are provided in a manner that makes the SSN easily redacted if released to the public." [3]

See References, Slide 17

10

Section 35 Continued

5. Request a purpose when collecting a SSN

- Each local government agency must file a written copy of its privacy policy with the governing board of the unit of local government within 30 days after approval of the policy. Each employee should be aware of the existing policy. A copy should be available to each employee and the public. Employees must be notified of any changes to the policy and a new copy must be readily available to the public.
- Each local government agency must apply the components of its identity-protection policy that are necessary to meet the requirements of this Act within 12 months after the policy is approved." [3]

See References, Slide 17

11

Best Practices for Prevention

- Do not leave voicemails containing SSNs
- Do not fax documents with SSNs to public fax machines
- Report any lost documents that contain SSNs
- Limit who can look at or use SSNs
- Protect devices storing SSNs by using encryption
- Collect only information that is task related
- Try to refrain from storing SSNs.
- Lock documents that contain SSNs [4]

See References, Slide 17

12

Disposing Confidential Information

- Contact "Central Repository" for approval before destroying any items.
- Check for confidential information before disposing documents.
- Shred confidential information or put it in a confidential waste bag.
- Cut or rip pieces that are ½ inch on all sides.

- Follow your district's confidential disposal policy .
- Do not shred documents in a public place.
- Destroy confidential information that is no longer required such as DVDs, CDs, USBs, PCs, and Laptops.[5]

See References, Slide 17

13

When to Give Out Your SSN

You're only *required* to give out your SSN in specific circumstances:

- Filing income taxes
- Entering into a new job
- Running business through financial organizations
- Applying for government benefits
- Applying for a driver's license [6]

See References, Slide 17

14

Violation

- Any person who intentionally violates this Act is guilty for Class B misdemeanor. [4]

See References, Slide 17

15

The End!!!

- Please proceed with completing the quiz for this training presentation.

16

References

California State University, Long Beach

- http://daf.csulb.edu/offices/vp/information_security/docs/ [1]

Illinois Identity Protection Act/ University of Illinois

- http://www.ssn.uillinois.edu/illinois_identity_protection_act__ipa__awareness/ [2]

Illinois General Assembly

- http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3174&ChapterID=2 [3]

Identity Protection Act Training

- https://www.csu.edu/compliance/pdf/identityprotectionacttraining.pdf [4]

Derbyshire County Council

- http://www.derbyshire.gov.uk/working_for_us/data/how_to_dispose_of_confidential_information_safely/default.asp [5]

US News

- http://money.usnews.com/money/personal-finance/articles/2013/07/01/when-to-give-out-your-social-security-number-and-how-to-protect-it [6]

See References, Slide 17

17