

Chapter 12

Regulatory and Policy Compliance with Regard to Identity Theft Prevention, Detection, and Response

Guillermo A. Francia III
Jacksonville State University, USA

Frances Shannon Hutchinson
Jacksonville State University, USA

ABSTRACT

The proliferation of the Internet has intensified the identity theft crisis. Recent surveys indicate staggering losses amounting to almost \$50 billion incurred due to almost 9 million cases of identity theft losses. These startling and apparently persistent statistics have prompted the United States and other foreign governments to initiate strategic plans and to enact several regulations in order to curb the crisis. This chapter surveys national and international laws pertaining to identity theft. Further, it discusses regulatory and policy compliance in the field of information security as it relates to identity theft prevention, detection, and response policies or procedures. In order to comply with recently enacted security-focused legislations and to protect the private information of customers or other third-party members, it is important that institutions of all types establish appropriate policies and procedures for dealing with sensitive information.

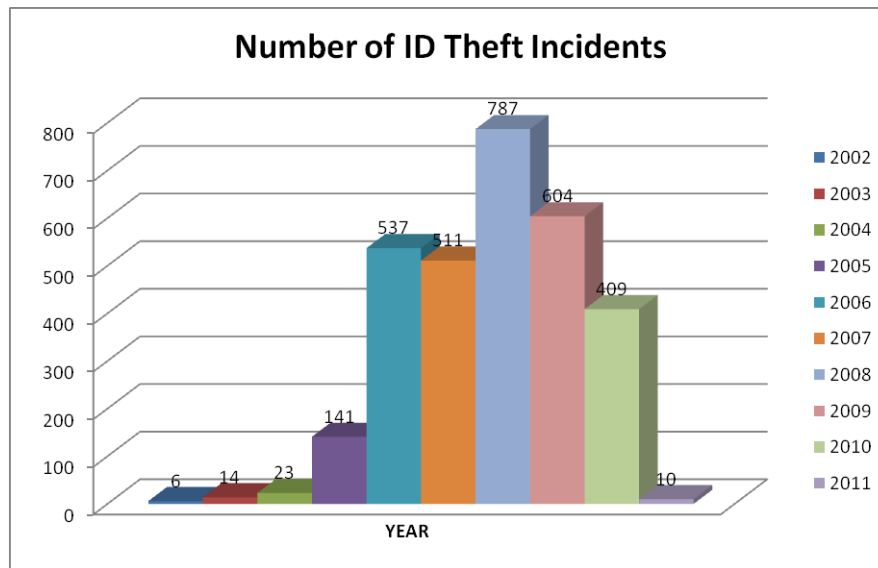
INTRODUCTION

This chapter discusses regulatory and policy compliance in the field of information security as it relates to identity theft prevention, detection, and response policies or procedures. In order to comply with recently enacted security-focused

legislations and to protect the private information of customers or other third-party members, it is important that institutions of all types establish appropriate policies and procedures for dealing with sensitive information. Listed here are certain laws which must be considered when developing identity theft related policies; guidelines for creating, implementing, and enforcing such policies are also cited.

DOI: 10.4018/978-1-61350-507-6.ch012

Figure 1. Annual ID Theft Incidents



BACKGROUND

Identity theft is a threat that has confounded society since the biblical times. The ubiquity of the Internet and the convenience of electronic transactions have exacerbated the threat and made it even much easier to execute. Recent surveys indicate staggering losses amounting to almost \$50 billion incurred due to almost 9 million cases of identity theft losses. A snapshot of several alarming statistics, which are gathered from the Open Security Foundation's DataLossDB (DataLossDB, 2011), pertinent to identity theft is shown in Figures 1 and 2. Figure 1 depicts the frequency of ID theft occurrences each year. As of February, 2011, there are already 10 incidents that involved ID theft.

Figure 2 shows the Personally Identifiable Information (PII) data loss categorized by data type in 2010. The data types are Date of Birth (DOB), Credit Card Number (CCN), Medical/Health information (MED), Social Security Number (SSN), Name and Address (NAA), and other miscellaneous information (MISC).

These startling statistics and their perceived persistent nature have prompted the federal gov-

ernment to initiate a strategic plan and several regulations to curb the crisis. We begin with the definition of important concepts pertaining to regulatory compliance and identity theft.

Definitions

Regulatory Compliance: A goal set by an organization in its attempt to comply with all laws or regulations relevant to that organization.

Policy Compliance: A goal set by an organization in its attempt to encourage and achieve compliance by its members/employees with regard to the organization's policies

Personally Identifiable Information: Any personal information by which an individual may be identified (SSN, bank account number, username/password combination, etc.).

Identity Theft: The co-option of another person's personal information without that person's knowledge and the fraudulent use of such knowledge (Princeton University, 2010)

29 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/regulatory-policy-compliance-regard-identity/61229

Related Content

Three Models to Measure Information Security Compliance

Wasim A. Al-Hamdani (2009). *International Journal of Information Security and Privacy* (pp. 43-67).

www.irma-international.org/article/three-models-measure-information-security/40360

Developing a Theory of Portable Public Key Infrastructure (PORTABLEPKI) for Mobile Business Security

Sashi Nand (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 1062-1069).

www.irma-international.org/chapter/developing-theory-portable-public-key/23143

Geopolitical Security, Technology, and Business Strategy: How Should Business Approach Geopolitics?

Josef Demergis (2025). *Security and Strategy Models for Key-Solving Institutional Frameworks* (pp. 1-20).

www.irma-international.org/chapter/geopolitical-security-technology-and-business-strategy/380667

Real-Time Cyber Analytics Data Collection Framework

Herbert Maosa, Karim Ouazzaneand Viktor Sowinski-Mydlarz (2022). *International Journal of Information Security and Privacy* (pp. 1-10).

www.irma-international.org/article/real-time-cyber-analytics-data-collection-framework/311465

An Australian Longitudinal Study Into Remnant Data Recovered From Second-Hand Memory Cards

Patryk Szewczyk, Krishnun Sansurooahand Patricia A. H. Williams (2018). *International Journal of Information Security and Privacy* (pp. 82-97).

www.irma-international.org/article/an-australian-longitudinal-study-into-remnant-data-recovered-from-second-hand-memory-cards/216851