

How to Use This Manual

We all know that identity theft is more pervasive now than it was 15 or 20 years ago. What we don't know is how to slow it down dramatically or stop its occurrence altogether. The federal government and certain federal agencies, such as the Federal Trade Commission (FTC), along with the FBI, the United States Secret Service, and the United States Postal Service, work together to investigate identity theft. They appear to be making some progress as the Department of Justice has increased the number of prosecutions substantially. Besides the efforts of the public sector, though, the President and government agencies expect the private sector to contribute to the prevention of identity theft by protecting their customers' identifying information.

When a thief makes a purchase with a stolen identity, corporations are now the victim of identity theft as well. Corporations are obligated, like all other organizations that collect customer financial information, to protect their customers' identities from theft. Corporations can use a variety of methods to safeguard customer information and reduce the risk of loss from identity theft, including:

- Verifying personal information to establish the identity of individuals purchasing products and services
- Establishing adequate procedures to detect possible fraud in new accounts
- Verifying the legitimacy of change of address requests on existing accounts
- Maintaining adequate security standards

One set of guidelines available are the final rules provided by the FTC, the agency associated with the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act. Although this rule refers to banks and creditors, the guidance it offers is suited for corporations as well. Corporations must have a program to prevent the theft of customer's identifying information by addressing the risk to its customers, its reputation, and its legal liabilities.

The *Corporate Guide to Identity Theft Prevention* can assist you in your efforts to protect the integrity of your customer information and to identify and monitor for signs that access to your information is at risk.

ORGANIZATION OF THE MANUAL

Chapters 1 through 4 concentrate on the underlying issues of identity theft.

Chapters 5 through 9 concentrate on federal requirements, other recommended practices for protecting customer information, and preventing information breaches. Chapter 9 provides policies and procedures related to verifying your customer's identity, response to computer breaches, information security, and for other relevant topics.

Chapters 10 through 12 address specific transactions that are prone to fraud thereby likely to be instrumental in identity theft. These three areas are of particular concern to businesses: the use of ACH transactions, credit card fraud, and ATM and debit card fraud.

By understanding the ACH system, a corporation can identify and address the risk of identity theft. For example, your organization is considered a corporate originator of an ACH transaction if you have been authorized to debit or credit the account of a customer. Chapter 10 is devoted to corporate originators of ACH transactions.

Credit card fraud can be perpetrated in various ways and there are state and federal laws that govern this area. Businesses need to understand what responsibilities the cardholder has for a transaction, what the merchant is responsible for, and what the issuing bank, or your organization's bank, is responsible for. Chapter 11 discusses credit card fraud.

ATM and debit card fraud can range from simple schemes, such as dishonest merchants retaining information from checks at the time of conversion into an electronic transaction to sophisticated skimming devices that capture information from debit cards at the time of use. Again, businesses need to be familiar with the responsibilities of each party to the transaction. Chapter 12 covers ATM and debit card fraud in the context of electronic fund transfers.

The final tab and its contents contain the Identity Theft Red Flag Toolkit. This toolkit contains a step-by-step guide to help your organization develop an ID theft prevention program. It also contains a Risk Assessment Worksheet to apply to the different departments of your organization, and sample policies and procedures.