Abstract

This chapter discusses the latest innovations in fraud detection, with a particular focus on insider fraud and organized fraud. It argues that as fraud continues to grow at an alarming rate across the financial services sector, the constant evolution in fraudster behavior means that financial institutions need to keep their technology-based countermeasures constantly updated, particularly given the increasing involvement of serious organized criminals. In addition to upgrading their current operational detection systems, this chapter aims to encourage organizations to improve current levels of data and information assurance in order to ensure the generation of high quality intelligence on the enemy, and to adopt a structured framework for better understanding and describing exactly what we mean by “intelligence.”

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Introduction

The Ongoing Fight against Financial Crime

Fraud continues to grow at an alarming rate across the financial services sector. According to the PricewaterhouseCoopers’ 2005 Global Economic Crime Survey, 45% of companies worldwide have fallen victim to economic crime in the past two years—an eight percentage point increase on the previous survey. Since 2003 there has been a 71% increase in the number of companies reporting cases of corruption and bribery, a 133% increase in the number reporting money laundering, and a 140% increase in the number reporting financial misrepresentation. Fraud that led to a loss of assets cost companies—on average—more than $1.7 million (U.S.), a 50% increase over 2003 (PricewaterhouseCoopers International Ltd. (PwC), 2005).

Identity fraud is a key growth area, having been labeled by federal and state authorities alike as the United States’ fastest-growing white-collar crime since the late 1990s. The Federal Trade Commission’s (FTC) 2004 report on identity theft revealed that consumer-reported losses from fraud exceeded $547 million. Identity theft topped the list of complaints for the fifth successive year, accounting for 39% of consumer fraud complaints (Federal Trade Commission (FTC), 2004). As for the future, Frost and Sullivan’s 2005 World Credit and Debit Fraud report predicts global losses to card fraud will reach $15.5 billion in 2009, much of this fueled by identity fraud (Frost & Sullivan, 2005).

In addition to those losses, there are also the costs of implementing antifraud processes and systems, not to mention lost opportunity costs. Furthermore, in the wake of serious fraud incidents, many companies suffer significant “collateral damage,” such as loss of reputation, decreased staff motivation, and declining business relations. Fraud also undermines the confidence of consumers in the system. Victims of phishing scams, for example, are becoming increasingly reluctant to use Internet banking or indeed engage in any kind of online financial transaction to the general detriment of the online industry.

Money laundering is a closely related issue, since the money gained from a successful fraud is by definition “tarnished” and may need to be laundered in order to make it easier to spend or invest. The magnitude of money laundering is difficult to quantify, the best effort to date being a 1996 International Monetary Fund (IMF) working paper that estimated the total amount of money laundered annually to be 2-5% of the world’s gross domestic product, or between $800 billion and $2 trillion (U.S.) in today’s terms (Quirk, 1996).

Worldwide, regulators are increasing the pressure on the financial services industry to reinforce their counter-fraud and counter-money laundering intelligence strategies and integrate them more tightly within their operational risk frameworks. From the U.S. Patriot and Sarbanes-Oxley acts to the EU 3rd Anti Money Laundering Directive and the UK Proceeds of Crime Act, the regulatory environment is increasing the liability of the institutions and the personal liability of their officers.

In light of these risks, financial institutions have devoted considerable resources to detecting fraudsters and other financial criminals through the more effective use of technology. Over the past decade, there has been an increasing take up of computer systems that examine transaction data and look for telltale patterns that might reveal potentially suspicious be-

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Analyzing the Existence of the Day of the Week Effect in Selected Emerging Country Stock Exchanges
[www.igi-global.com/article/analyzing-the-existence-of-the-day-of-the-week-effect-in-selected-emerging-country-stock-exchanges/119401?camid=4v1a](www.igi-global.com/article/analyzing-the-existence-of-the-day-of-the-week-effect-in-selected-emerging-country-stock-exchanges/119401?camid=4v1a)