

People, Process and Proprietary Information:

The Three P's to Preventing Fraud

www.sitel.com

In This White Paper

- Thanks to Sarbanes-Oxley, CEOs and CFOs are now held accountable for the effectiveness of the initiatives their companies have in place to detect and prevent fraud. What are you doing to ensure your service provider is on top of this?
- Background checks are an effective way to ensure the people you have dealing with your customers are a reliable fit for your business.
- Having adequate processes in place - including the controls over access to the Intranet and other electronic communications - should be a key part of your fraud prevention strategy.
- Tracking access and use of proprietary information and creating an electronic audit trail will help ensure a quick and easy investigation when it is needed.

Introduction

“As more companies elect to outsource various business processes, they must also ensure their outsourcing partner is taking the necessary precautions to detect and prevent fraud.”

No matter what form it takes, fraud can have devastating, lasting effects on a business—from hefty fines and sanctions to irreparable damage to company reputation. Financial services firms represent a particularly attractive target for fraudsters because of the sensitive, valuable nature of the information contained within their databases. Thanks to the Sarbanes-Oxley Act of 2002, CEOs and CFOs are now held accountable for the effectiveness of the initiatives their companies have in place to detect and prevent fraud. As a result, it is imperative that organizations bolster their internal controls. As more and more companies elect to outsource various business processes, they must also ensure that their business process outsourcer (BPO) is taking the necessary precautions to detect and ultimately prevent fraud. To determine if a BPO has proper fraud prevention techniques in place, an organization must ensure that the “three P’s” of fraud prevention are secure:

1) People

Documenting and carefully monitoring employees who are privy to sensitive customer information is an essential first step toward fighting fraud. For financial services firms that outsource, it is important to understand which call center agents have access to credit card numbers, debit card numbers, bank account information, Social Security numbers and dates of birth.

When selecting an outsource partner, companies must demand that background checks be conducted on all employees to determine their reliability. What’s more, the term “background check” must be clearly defined because it can refer to a number of different procedures. It should mean a complete criminal check on the county level using an address history from a Social Security number trace. For employees who are conducting bank transactions, it is also critical to conduct a federal-level criminal search as well as a Financial Institutions Reform Recovery and Enforcement Act (FIRREA) Restriction List check.

Other aspects of an efficient background check include compiling an employee's credit history as well as conducting personality inventory testing. If these processes are incorporated into the hiring process, companies can be assured that those employees who have access to sensitive information are completely reliable and fit to handle the responsibility.

2) Processes

In addition to ensuring the hiring of reliable employees, financial services firms must evaluate the processes that potential BPOs have in place to secure against identity theft. This includes: identifying all incoming sources of customer personal information, tracing the flow of this information and identifying the locations where the information is most susceptible to theft.

One example of a poor process that many contact centers have in place is unrestricted agent access to the Internet. Many call center applications require Web access, but having access to financial services firms' customers' information without restrictions on Internet use is a recipe for disaster. Agents' workstations should be locked down so they can only access the Web sites required to perform work-related functions. This will restrict access to sites—including chat rooms or Web-based email sites—that would allow the transfer of customer information from the workstation.

Another process that BPOs should have in place is the prohibition of cell phone use on the call center floor. Mobile phone conversations cannot be monitored or recorded and therefore represent a potential asset to fraudsters. The continually advancing capabilities of cell phones also represent a concern—including the sophistication of camera functionality and increased storage capacity.

3) Proprietary Information

The Payment Card Industry (PCI) data security standards require that all access to credit and debit card information—even view-only access—be logged and an audit trail created. The best way to comply with PCI and protect proprietary information in the call center is to have a paperless workstation. Nothing should be handwritten; it should all be entered directly

into the desktop. When a credit card fraud takes place, it is critical to determine the identity of the last employee to view the card record. When financial services firms cannot report who may have viewed customer information, the investigation is prolonged.

Summary

Outsourcing is a valuable asset to the financial services community. The right partner can offer a lower cost structure while still adding business value and generating revenue. However, before selecting BPO, companies must ensure that the three Ps are secure and thorough, effective controls are in place to detect and prevent fraud. The success of any business depends on it.

About Sitel

Sitel is a global Business Process Outsourcing (BPO) leader that meets clients' customer care and transaction processing needs by providing world-class solutions from over 60,000 associates in 155+ facilities located in 27 countries.

Sitel provides clients with the strategic insight, scale and diversity of offerings to ensure the best return on their customer investment. For more information, please access www.sitel.com



*Two American Center
3102 West End Avenue, Suite 1000
Nashville, TN 37203
USA*

+1 866.95.Sitel