Rapidly Address Compliance Gaps

Non-Intrusive Technology
to Police the User Desktop;
Fast Implementation and Returns

openspan

Rapidly Address Compliance Gaps
Non-Intrusive Technology to Police the User Desktop; Fast Implementation and Returns

INTRODUCTION: **285m Transactions at Risk for Fraud**

Last year, around 285 million credit or debit card transactions were at risk for fraud, according to the security firm Veritape, which performed in-depth research on security risk at UK call centres. One glaring finding was a lack of knowledge – let alone corrective compliance – that contact centres must erase each and every recorded instance of payment card security codes processed by their agents and agent software applications.[1]

There are many similar gaps resulting from the mismatch between an increasing number of compliance requirements on one hand, and the way line-of-business software applications can help execute them. This paper examines some common cases and then describes currently-deployed solutions that control, modify, and extend existing software applications to meet those challenges.

COMMON CHALLENGES

Compliance requirements are being continually added to businesses due to more government laws and regulations, trade association guidelines, and through evolving business process adherence rules. Some examples include:

:: **Recording / Fiduciary Security.** Contact centres increasingly employ recording technology, both voice and desktop, for reasons ranging from analysing call metric analytics to agent coaching. The current Payment Card Industry (PCI) Data Security Standards (DSS) guide lines don't mention security of recordings, but according to the same security standards, card validation codes and values require the highest level of security and safeguarding. Recording other data such as Primary Account Numbers (PANs), cardholder names, addresses, and transaction information should be guarded as well.

:: **Mandatory disclosures.** Many transactions require mandatory disclosure of national, local, or other jurisdictional information to consumers by the agent. That information may be oral or in writing, and could require certain kinds of customer acknowledgements or confirmations.

:: **Telephone Preference Service, Do Not Call lists.** These national opt-out registries have rigid adherence requirements, and compliance violations can result in fines of £5000 per call. Consumer record information, including phone numbers, is often distributed amongst multiple agent desktop applications such as CRM, mainframe, payment, and others.

:: **Account servicing.** Users should be limited from certain actions except within specified criteria, such as changing credit limits or performing transactions such as charge-backs or other adjustments for a certain amount.

---

[1] As cited by Coney, James. "Phone Shopping Puts Card Details Of Millions At Risk As Fraudsters Target Call Centres." Daily Mail Online, 16 October 2009. http://www.dailymail.co.uk/news/article-1220731/Phone-shopping-puts-card-details-millions-riskas-fraudsters-target-centres.html

:: **Business process adherence.** Users of all experience levels can become lost whilst flipping between multiple desktop application windows and often resort to hand-written checklists and the like to execute critical, complex tasks. On-boarding and provisioning may require letters, contracts, agreements, welcome lists, or other physical (e.g. plastic credit cards, access keys) or email items generated and sent. A business-to-business transaction might include complex inventory, shipping, receiving, and billing actions.

:: **Data access based on role or transaction.** This would be beyond first-tier solutions such as sign-on security. For example, interfaces might need restricted data fields flexibly if not dynamically masked, but this could prove difficult without a costly and lengthy services solution.

Most line-of-business software applications are not engineered to solve these problems without extensive modification that involves invasive code and architecture changes or a "rip-and-replace" approach that still may leave newer applications isolated from legacy systems.

OPENSPAN COMPLIANCE SOLUTIONS

The OpenSpan Platform can monitor the desktop environment to intercept multiple events spanning multiple applications and then actively alert managers, change application behaviour, or assist in business process improvement, adherence, and compliance.

The following examples illustrate ways that OpenSpan is currently deployed to non-invasively extend, join, and task-automate existing desktop applications to solve common compliance complications.

:: **Recognise prohibited actions, trigger automations to restrict and report.** One OpenSpan partner solution records both user voice and desktop actions; OpenSpan intercepts the most granular desktop events to pause recordings at the precise moments that PCI DSS-restricted data such as validation codes and values are passed, while leaving the recording technology's full tagging and retrieval completely functional.

:: **Restrict screens and fields non-invasively.** OpenSpan lets you augment current security and access programs by selectively masking and modifying existing user interfaces to display or process only the information required. One example would be removing personal customer data from bank teller interfaces without costly modification to a legacy branch banking platform.

:: **Ensure business process completion.** OpenSpan solutions extend traditional BPM to the desktop by ensuring that multiple events spanning multiple applications are monitored and checked for proper completion. One example is accessing the proper mandatory legal and regulatory advisories for a given transaction, ensuring that they have been communicated to the customer, and recording that confirmation. OpenSpan automations in contact centres integrate case journaling with dynamically-generated references and statements.

:: **Initiate documentation or provisioning workflow.** Many transactions, particularly financial, require physical instruments – letters or forms generated, printed, and emailed, faxed or sent through the National Post to the customer. OpenSpan solutions are deployed that produce and send required fulfilment documentation or provisioning materials based on an agent or event trigger.

:: **Monitor and Control Account Interfaces.** OpenSpan's real-time intercept-and-react capability is extremely powerful and can be used to alert management of or even stop many kinds of potential compliance violations from being executed by the user, no matter whether accidental or deliberate.

:: **Validate data.** OpenSpan can ensure that information entered is current and accurate. Examples include validation of addresses and credit scores from external agencies that are returned to an agent in real time.

:: **Synchronise data between desktop applications and with enterprise systems.** OpenSpan can integrate a suite of disparate agent desktop applications and automate data synchroni- sation. For example, if an agent has to access a 3270 system for account master records, a main Win 32 CRM application, and a SaaS Web application for credit verification, the data can be consistently synchronised between those applications; further, if the agent updates information in one window, the data is pushed to all other relevant applications automatically.

THE OPENSPAN PLATFORM

OpenSpan is not another additional application. Instead, OpenSpan helps organisations improve the performance and productivity of customer-facing staff and other knowledge workers using the applications and systems already in place. OpenSpan makes your existing applications smarter – allowing you to rapidly integrate, automate and extend your applications and the business processes that span these applications.

OpenSpan's integration and task automation is possible between any of the following:

:: Windows and other client/server applications
:: Host applications
:: Web applications including Web 2.0-style applications
:: Java applets and applications
:: Software-as-a-Service or third party applications where you might not have access to source code
:: "Closed" or custom-built applications with no available API or connector
:: Web services (SOAP, REST, HTTPS, etc.)
:: Virtualised, including Citrix-streamed applications
:: Any application that ultimately gets delivered to a user using a Windows operating system

This is especially valuable within any enterprise or institution with a heavy concentration of older legacy and large platform applications.

SUMMARY

While compliance requirements – and penalties – continue to multiply and grow, business software applications, whether cloud, legacy mainframe, Windows-native, virtual, or others, will largely not come pre-configured to efficiently solve common compliance issues. Doing so could require services contracts with large potential costs in terms of time and money both initially and going forward.

But as a proven alternative, the OpenSpan Platform provides non-intrusive application integration and task automation that's more flexible and faster to implement and commonly provides returns faster than other solutions. It is in use around the globe solving a wide range of compliance issues for clients in customer-facing and back-office roles in many different public and private concerns.

GET MORE INFORMATION

To learn more, browse other OpenSpan case studies, white papers and online demonstrations by visiting **www.openspan.com, or contact us at the address below.**

openspan

OPENSPAN EMEA
ALPHA HOUSE
100 BOROUGH HIGH STREET
LONDON SE1 1LB
UNITED KINGDOM
PHONE: **+44 (0) 203 005 7592**
EMAIL: SALES@OPENSPAN.COM