

The Seven Deadly Sins of Payments

[Matt Chan](#), [webMethods](#) - 25 Oct 2005

By addressing the seven deadly sins detailed in this article, banks can streamline their payments business end-to-end, eliminate costs from processes and deliver differentiated services that warrant premium pricing.

With payments processing offering minimal levels of differentiation, wholesale banks are often left to compete on price, which forces them to continually improve their efficiency despite the need to also maintain or improve their service levels. In fact, corporate customers are even adding demands for banks to provide real-time insight and greater transparency over their payments transactions. These challenges are compounded by today's growing regulatory requirements, which add extra costs and operational burdens that further decrease margins.

Fully automating the payments process to eliminate extraneous costs has long been the industry's mantra and must remain so. However, in order to truly counter the ongoing erosion of transaction fees, successful institutions must also accept the need to fully leverage these process automation investments to deliver additional, value-added services as well. Besides offering richer, more accurate payment information, banks can (and must) expand their offerings to include new services that are enabled by a fully automated, end-to-end process. These can include payments netting, inward payments discounting, and the coupling of foreign exchange transactions. Fortunately, most corporate customers are willing to pay for these additional services.

So, what's preventing banks from achieving this desired state of nirvana? Beyond the typical issues faced in managing complex global institutions, analysis of their payments operations reveals these common stumbling blocks:

1. Fragmented, redundant operations where process steps are unnecessarily duplicated numerous times.
2. Frequent manual interventions that introduce preventable process bottlenecks.
3. Ad-hoc and error-prone exception handling that not only fails to follow a consistent remediation procedure, but is often undocumented as well.
4. Too many access points to critical applications and dispersed information when trying to resolve customer issues.
5. Lack of real-time visibility into system failures and their associated business impact which jeopardizes a bank's ability to meet service-level commitments to key customers.
6. Unpredictable system failures that often result in a bank treating the symptoms, not the cause.
7. Failure to fully leverage existing investments and technology to satisfy regulatory compliance needs.

Fragmented, Redundant Operations

Most banks do not holistically manage their payments businesses. Instead, they operate each business as autonomous or close-to-autonomous silos - each with its own processes, applications, and IT infrastructure. These redundancies limit the bank's ability to react to competitive threats and raise the cost of operations (business and IT). Leading institutions have begun to centralize and consolidate their payments strategy to secure better bottom-line insight into their payments business.

Tangible economies of scale have been achieved through the rationalization of systems and applications and through the adoption of service-oriented architecture (SOA) to promote the reuse of IT assets. For example, most payments products have a 'balance inquiry' step in their system processes, and each payments silo, most likely, has coded this step separately and differently. With a SOA approach, this 'balance inquiry' step can be coded once and reused by any business process that needs it - dramatically lowering the cost of operations and system maintenance. Multiply this by the thousands of steps and sub-steps typically used within a bank's processes and the savings add up quickly.

Frequent Manual Interventions

Banks have made great strides to automate many of their payments processing steps. However, due to the proclivity for mergers and acquisitions in this industry and the resulting disjointed organization structure that they produce, there is still too much human intervention - creating unnecessary business bottlenecks. The obvious first step towards eliminating these bottlenecks is to identify them. While most banks have some form of institutionalized processes, they often need to visually model their entire processes on an end-to-end basis so that both system and human touch points can be clearly identified. The next step is to determine if all of the human touch points are required. For the required ones, assess if they can be performed automatically by systems and applications. If so, support IT initiatives to systematize those human touch points.

The final step is to implement a business process management (BPM) tool to orchestrate these critical processes - for example, tracking all payment transactions flowing through the institution at any given time and noting any exceptionally long delays.

Ad-hoc, Error-Prone Exception Handling

The reality is that not all human interactions in the business process can be automated or systematized, especially when exceptions occur. In such instances, humans (usually more senior employees) have to intervene to make decisions or authorize payments. Sometimes these decisions are made based on personal judgment or in the absence of clear policy - all of which contribute to errors in payments processing that can produce countless hours of re-work and endless customer frustration. In some instances, these human errors can put the bank at risk of violating compliance mandates. To mitigate these risks, a bank can incorporate workflow systems into their payments processes. Workflow systems allow the bank to institutionalize remediation procedures that supersede ad-hoc human judgement with pre-approved criteria encompassing all relevant information. Also, a workflow system provides the bank with an audit trail documenting the who, what, when, where, and how of any human decision. Who made the decision? What problem was resolved? When did it occur? Where did it occur? And how was the decision derived?

Too Many Access Points to Critical Applications

When a payment problem occurs or a customer simply calls to inquire about the status of their payments, additional human intervention is required. Too often, the disparate nature of this information, where it is either spread across multiple applications (e.g. CRM, core applications, posting systems) and has to be compiled or it is not synchronized and up to date, means that this customer cannot be quickly or fully assisted. At some institutions, employees spend up to 25 per cent of their time looking for information needed to perform their job functions. Consequently, the institution suffers from additional lost productivity, fails to fully leverage their investments in packaged applications, and is driven to make decisions based on incomplete information. To remedy this situation, banks have begun to deploy 'composite applications' that draw upon the capabilities of a collection of existing applications to deliver more complete views of information specific to the task being performed by the employee. This not only helps the institution to improve the return on investment (ROI) realized from their package applications, but it also improves their responsiveness in resolving customer issues, which further lowers their cost of operations.

Lack of Real-time Visibility into System Failures

Leading banks have invested significantly in their IT infrastructure. Their IT organizations have implemented redundant systems and deployed monitoring tools to alert them if a server, application, or network goes down day or night. This type of operational visibility ensures that system outages are addressed as quickly as possible. But it does not provide line-of-business (LOB) leaders with the visibility or other resources needed to address the resultant business problems. For example, lack of correlation between hardware components and the process steps that they support mean that administrators are challenged to immediately determine the business ramifications of a disruption. By providing LOB leaders with visibility into which payments process or business is impacted when a system failure occurs, they can take immediate corrective actions to manage the business risks associated with this event and are more likely to meet their customer commitments. These actions could be as simple as manually processing the critical transactions or contacting the affected customers to alert them of a possible delay in their payments transactions while re-assuring them that the bank is employing all available resources to address the situation.

Unpredictable System Failures

Real-time visibility into system failures and their associated business impact is immensely valuable. However, the better scenario is to anticipate these failures and address them before they can negatively affect the business. A select number of banks have adopted tools that create 'data fingerprints' to better understand the pattern of system behavior that contributes to system failure. As a result, these self-learning tools can then predict a potential problem based on the real-time monitoring of data metrics that contribute to the formation of the pattern. As more adverse data metrics are detected, the confidence level of the prediction increases - allowing the bank to prevent business problems from occurring and fix the root cause(s) contributing to the system problems.

Failure to Leverage Existing Investment

Satisfying compliance requirements is one of the most expensive investments in the banking industry. In an environment where there is constant pressure on fees and competition is high (like payments), banks are keeping a close watch on margins. At the same time, the high cost burden of compliance is placing a tighter squeeze on margins. Some of the more pragmatic banks have realized that their existing operational investments can also be leveraged to satisfy compliance requirements. For example, banks have leveraged their BPM and real-time monitoring tools to fulfill and document compliance measures. When business processes are orchestrated by BPM, human interactions are managed by workflow, real-time business visibility is available, and problems can be predicted, banks have all the tools to manage their operations to comply fully with corporate policies as well as regulatory mandates - all while leveraging the same investments.

By addressing these seven deadly sins, banks can fully streamline their payments business end-to-end. In doing so, they eliminate costs from processes that hinder their competitiveness while delivering new, differentiated services that warrant premium pricing.