



A Premier Publication Dedicated to Bringing You the Latest  
Top Tier Technology Articles, Trends and Views in the Industry.

## Vertical Focuses

Education  
Finance  
Government  
Healthcare  
Industrial  
Life Science  
Manufacturing  
Medical  
Pharmaceutical  
Wireless

## Horizontal Focuses

2010 Award Winners  
Automation  
CRM  
DAM  
Data Mgmt.  
EHR  
ERP  
Mobile Devices  
PLM  
SAAS  
Software

## Code of Ethics

Awards

## 2010 Award Winners

### Bermuda Commercial Bank Invests in People, Technology and Customers

*The one/two punch on mitigating risk and achieving  
banking compliance*

By Drew Barrows

In a tumultuous economic environment, risk and compliance practices are more important than ever. Globalization has changed the way many businesses operate. As their marketplace swells and diversifies with a growing number of channels and cross-border transactions, risk management and compliance have become top strategic priorities for many banks.

The situation has been intensified by crises in financial markets around the world. This is why banks are finding it imperative to deploy better and more cost-effective strategies to mitigate financial crime and meet regulatory requirements. For instance the [Bermuda Commercial Bank Limited \(BCB\)](#), the only bank in Bermuda that is focused solely on commercial, corporate, fund, and private wealth individuals, deemed it necessary to develop a robust compliance practice that maintains the security of their funds, as well as the funds of their customers. Part of BCB's strategy is that it is pro-active, pre-emptive and hands-on in safeguarding its business, its funds and servicing its customers.

"We have a clear vision on the way we like to do business and part of that vision entails understanding the importance of balancing compliance and risk without sacrificing the quality and responsiveness of our services," says Horst Finkbeiner, Director and COO of Bermuda Commercial Bank. These "moments of truth" represent important opportunities for banks to assess their customer service capabilities and to ensure a proper alignment of investments with customer needs as BCB has long been prudent in doing without compromising the strength of the banks compliance and risk policies. Bad customer service experiences often translate to lower balances and lost business for banks. And typically banks will turn to automation and technology to improve upon the customer's banking experience while mitigating risk and ensuring compliance. BCB is implementing [Misys' BankFusion](#)

Universal Banking and has enhanced its customer service experience as well as expanded its product portfolio and banking services. Misys' in-depth global knowledge of connectivity to SWIFT complements EastNets' real-time transaction monitoring and SWIFT reporting solution used by BCB. BankFusion provides a systematic roadmap for bringing new products to market more quickly and efficiently.

Banks have long recognized the advantages of deploying technology to improve the value, speed and flexibility of their product offering to customers. Particularly in today's highly competitive banking industry, bank technology is a vital element that can be used to help a bank differentiate itself. This is especially true on the retail front where banks tend to offer newer technology-driven channels to customers such as ATMs and Internet banking.

BCB is fully aware of the risks inherent in EFT, the electronic exchange or transfer of money from one account to another, either within the same financial institution or across multiple institutions in terms of pinpointing unusual transaction patterns or trends. "We have developed a straight-through processing environment that actually allows our team to utilize their better professional judgement and proactively react in real time to any unusual activity," says Finkbeiner. BCB applies a strategic approach that involves the automation of routine processes so that its people have the freedom to improve operations, reduce costs, and prepare for growth.

In order to protect their customers and the bank against fraud, BCB is proactive in training their staff on how to identify risks associated with EFTs and all banking transactions. BCB manages risk through a combination of an extremely conservative risk policy in balance sheet management in addition to applying robust compliance risk management technologies. The bank deployed the en.SafeWatch Profiling anti-money laundering application from EastNets as part of its automated central data processing, trend/pattern analysis and suspicious behavior identification processes. EastNets banking technologies supports the bank's transaction monitoring initiative. For instance, the bank utilizes EastNets' Watchlist Filtering solution primarily to routinely scan current and prospective clients against a database (watch list) consisting of names, aka and address entries.

The banking industry has entered a new era in Office of Foreign Assets Control (OFAC) compliance, recognizing that there is no one right way to monitor for OFAC

compliance when implementing a risk-based approach. BCB addresses OFAC, PEP (politically exposed person) and other regulatory lists screening using EastNet's real-time Filtering solution and SWIFT (Society of Worldwide Interbank Financial Telecommunication) reporting to meet compliance requirements. "BCB's sophisticated OFAC screening and filtering technology quickly identifies any potential risks while limiting false positives," says Finkbeiner. "This strengthens and focuses our compliance practices saving us substantial time and money."

Thus far the banking industry has done a remarkable job of abiding by the many sanction programs administered by OFAC in the interest of enforcing U.S. foreign policy, as well as other official programs such as the Bank of England financial sanction list. The relatively small number of civil monetary penalties that OFAC has levied further illustrates the industry's solid compliance record. This is not to say that many low-risk community and regional banks are not challenged by the adoption of the 2005 standards. In fact, a large number of smaller institutions and a few regulators alike are struggling to apply the methodology of an enterprise-wide risk-based OFAC program to low-risk environments. "We are able to centralize in real time our SWIFT Traffic data, FIN and MX messages and events, in our database so that our staff accesses any statistical data they need at any time," continued Finkbeiner.

BCB, a member of the SWIFT network, integrates EastNet's SWIFT Alliance monitoring application within its existing SWIFT environment for conducting real time filtering of both its incoming and outgoing SWIFT messages. This is especially important to BCB because they have established correspondent banking relationships with major institutions around the world, allowing them to provide multi-currency wire transfer services globally. Additionally, EastNets' SWIFT Alliance monitoring application automatically and pro-actively prevents the emission of suspicious messages into the SWIFT Network. BCB also uses EastNets file connector application to scan the contents of large data text files irrespective of their size and formats and does parallel scanning to allow multiple scan processes and batch checking. The way it is configured allows the en.SafeWatch Filtering to work with almost any file format the bank uses. According to Finkbeiner, "our filtering and reporting capabilities have helped improve our overall operational efficiency through automatic reporting, and the ease of accessing real time data to do analysis, investigations and audits, in a fast and flexible way."

It is becoming evident that any financial institution offering EFT products and services to their customers need to have sound AML and CTF (Anti-money

Laundering and Counter Terrorist Financing) policies, procedures and processes in place to manage the risks associated with EFTs. Without these programs the risks of electronic banking can result in financial loss and reputation damage for the financial institution through fraud, disclosure of customer information or corruption of data. There are many warning signs of potential fraud that bank staff must be informed of and prepared for.

As more bank customers begin to use electronic banking solutions, hackers and money launderers are becoming more creative in their fraud tactics. Simply put, EFTs are subject to higher risk and exposure to fraudulent activities, and fraudulent activity is damaging to a financial institution's relationship with its customers. According to Finkbeiner's words of wisdom on the subject, "financial institutions must proactively invest in AML and CTF training and programs to better prepare their employees to identify the risks that may occur in processing transactions. We have made sure we have the right people in place and a highly qualified team working collaboratively together to mitigate risk and ensure compliance."