



John Geurts, Executive General Manager for Group Security

Fraud detection with a rapid return

Within months, Commonwealth Bank of Australia sees 95 percent increase in check fraud detection efficiency.

Industry

Banking

Business Issue

Detect fraud in all bank operations more efficiently.

Solution

SAS allowed the Commonwealth Bank to migrate all its siloed information onto one platform in order to analyze transactions and customer activity, develop new models and tune existing models to improve fraud detection efficiency, and create reports.

Benefits

The bank has detected twice the level of check fraud than in its legacy system, increased Internet banking fraud alerts by 60 percent, and check and Internet fraud loss-to-turnover ratios are 50 and 80 percent better, respectively, than five years ago.

Using SAS, the Commonwealth Bank of Australia has detected twice the level of check fraud than in its previous system and had a 60 percent improvement in Internet banking fraud-alert volumes.

John Geurts, Executive General Manager for Group Security and Chief Security Officer, offers his thoughts about Commonwealth Bank's use of SAS® and the importance of taking a unified look at financial crimes.

Banks often take a siloed approach to addressing fraud – check fraud is handled by one group, credit card fraud by another. The Commonwealth Bank has taken a single platform approach to address all financial crime, including money laundering. Why did you choose a platform approach?

Geurts: Financial crime is constantly evolving. Local and transnational criminal groups are very fluid in their structure and approach. Equally as important, the Commonwealth Bank provides a range of integrated financial services that include retail banking, private banking, business banking, institutional banking, funds management, superannuation, insurance and investment, and share brokerage products and services.

We adopted a platform approach because we needed a holistic view of fraud and financial crime that was independent of product, channel or geography. We were also looking to achieve an economy of scale, reducing data storage costs, enabling reuse across the group. In addition, we needed the flexibility to add new

products, services and channels to the platform at a far lower incremental cost than installing another customized fraud detection system.

An integrated approach also provides us with the data integrity and modeling sophistication that allows us to make substantial operational improvements in alert volumes, false-positive ratios and rate of fraud detected. We simply needed to be able to future-proof our fraud systems to adapt to any foreseen or unforeseen changes in our business requirements.

Did you migrate everything at once?

Geurts: No, we took a staged approach with our financial crimes platform and have migrated our siloed capability onto the platform, including: Internet fraud, internal (staff) fraud, application fraud, check fraud, merchant fraud and debit card fraud. We also use the platform to conduct the analysis required to get the best out of our credit card fraud system, which is provided by a bureau. And of course, transaction monitoring for anti-money laundering/counterterrorism financing compliance uses the same platform. This has saved us an enormous amount of data integration and data management rework.

How did you address the issue of staff malpractice or internal fraud, which is an area that you can't typically get from an "out of the box" solution?

Geurts: I must make it clear that we do not specifically monitor our staff's bank accounts, which is a common misperception. Our staff members are



THE
POWER
TO KNOW.

“The reduced loss ratios have translated to a real and substantial reduction in fraud loss expense for the Commonwealth Bank.”

John Geurts
Executive General Manager for Group Security
Commonwealth Bank of Australia

entitled to the same degree of privacy and protection that all of our customers receive. I believe we have a sophisticated approach that balances the need for privacy with the need to protect the group and our customers from internal fraud.

In the past, it felt a little like finding a needle in a haystack. We understood most of the methods of how one would commit such crimes, but it was almost impossible to detect who was perpetrating these acts without detailed data readily available. You are dealing with individuals who know and have access to the bank's systems and have an understanding of our internal control environment. This is the value of a platform approach, enabling sophisticated models and data mining to detect unusual behavior between our staff and single or multiple accounts held with the bank.

Internal fraud shares a number of behaviors with suspected money laundering and terrorist financing. So we need to look at a range of data sets that are not just related to bank accounts, an approach that requires a platform view. We also uncovered both check fraud and application fraud – you couldn't get this detection capability without a platform approach.

Did your aggressive goals for fraud detection present new challenges in terms of the data required?

Geurts: We initially underestimated the complexity of the task. The data previously available was never designed to assist us with what we were now looking to achieve. The level of aggregation and the availability of data were not appropriate. To overcome this, we needed to extract some data from the source systems, particularly for the bank's demand deposit system. We had to prioritize where to start, which system to address first, and so on. This was a huge undertaking but when I look back I realize that, in building such a significant asset to be leveraged by the Commonwealth Bank, getting the data right was critical.

What results are you seeing so far?

Geurts: Check-fraud detection efficiency has improved from a false-positive rate of one in 2,000 to approximately one in 100 – which is a 95 percent improvement, with a similar improvement in alert volumes. We are also detecting twice the level of check fraud in the SAS-based FCP [financial crimes platform]. We have achieved more than a 60 percent improvement in Internet banking fraud-alert volumes and are detecting a higher rate of fraud; we are consistently achieving a one to 12 false-positive ratio in our cards fraud-detection platform,

which again is better than industry benchmarks.

Most importantly, on an indexed basis, our check and Internet fraud loss-to-turnover ratios are 50 percent and 80 percent better, respectively, than five years ago, and our card fraud losses are marginally better. Given the sustained growth in business volumes in those five years, the reduced loss ratios have translated to a real and substantial reduction in fraud loss expense for the group since the FCP was implemented in July 2007.

What ROI did you achieve?

Geurts: We achieved very rapid benefits, within months, in terms of the efficiency of the rate of fraud detected as well as the financial benefit from retiring multiple legacy systems. As we've grown, we haven't had to add staff. The staff we have can handle the work with help from the SAS solution.

What did you learn from the experience?

Geurts: We need to access highly granular data at its source, that the system must be used for transactional analysis, modeling and data discovery, and that your implementation partner is important. SAS brought a significant amount of knowledge to this solution.



**THE
POWER
TO KNOW.**

SAS Institute Inc. World Headquarters +1 919 677 8000
To contact your local SAS office, please visit: www.sas.com/offices

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2009, SAS Institute Inc. All rights reserved. 103958_536839.0409