

# Dynamic Tension

Tom Groenfeldt

Migration to a new platform gave HSBC a chance to break down some silos without losing data

**“Dynamic tension” is how Sharon Allsop-Kenney describes her working environment as head of the Business Intelligence Competency Centre at HSBC in London.** Users want fast solutions, IT wants to protect the information environment, and architects think very long term about how it all should work together. Meanwhile banks’ profits are under pressure.

Speaking at the Teradata Partners Conference in San Diego, California early this month, she said that banking faces increasing demands from regulators, both locally and globally. In the UK, she added, it also faces an often hostile media.

“Banking is unpopular. We need to be very, very responsive to the needs to serve our customers well, and intelligence has a huge part to play in helping the organization meeting those demands and build out from what has been one of the worst economic situations we have been through.”

At HSBC, pressures on margins mean the organisation is under pressure to do more with less, she added – but not too much less.

In 2007 the UK retail and commercial divisions of the bank nearly ran out of computing power. The bank’s technology wasn’t keeping pace, it had a messy situation with split environments and different systems struggling to keep pace with customer demands. In 2009 the bank did a lift and shift to Teradata.

“The great news is the migration gave me a performant, stable and scalable environment. It was a hugely successful migration.” But if she had to do it again, she would prefer to clean up the complex and messy legacy data structures rather than just move them – “Although I don’t know that we had the time to make a different decision,” she said.

One job of the BICC is to keep data anarchy at bay. The BICC aims to create as close to a single version of the truth in as close to real-time as possible, although she admitted that a single repository isn’t going to hold all the bank’s data anytime soon. But when the bank does have multiple repositories, it wants to keep the data consistent across them.

A constant source of dynamic tension is the different desires of business and IT. The

business side wants fast implementation of solutions while IT serves as the guardian of a very structured environment which has to be protected. Silos and disparate platforms are often the result of business groups implementing a solution with no regard to the bank’s broader architecture and information requirements.

**“We had a complicated legacy of silos with business users providing their own data in data marts, data in handbags and data under their desks.”**

Allsop-Kenney said the BICC has a team that works closely with the business to understand its needs and guide the business users toward an effective solution which maintains data quality. When the goals are defined, project managers from BICC take over the development and implementation.

“That’s a great benefit because it gives me the opportunity to influence the project outcomes and keep them consistent with the strategy. The legacy was for business leaders to drive the project managers for the fastest solution.” That often was to create a silo which was very effective for the immediate business goal but walled off the data which could provide a broader view of the customer.

“We had a complicated legacy of silos with business users providing their own data in data marts, data in handbags and data under their desks. They have been doing that because we in the intelligence organisation have not been able to provide them with the solutions they need. This package of projects was put in place to provision that demand.”

She described the IT legacy at HSBC as a federated community of banks that bought their own systems. One department might have liked blue, another preferred pink, but no one considered how they would integrate.

“When we implemented BICC we

faced an estate of data silos. I am nowhere near getting rid of all those, but we have a program of projects in place to break down the silos and move data into the core repository. We do it when there is a clear cost benefit.” She takes budget wherever she can find it, including from security because a data loss would be catastrophic.

The BICC has developed a data lab where business users can see if moving their data into Teradata brings the benefits they anticipated. They have approximately 90 days to work with the data in the data warehouse and link it to other data to look for business value. They still have to pay the cost of moving into production, but the lab at least gives them the opportunity to develop a business case for the warehouse approach.

The bank needs all of its customer information to manage risk, liquidity and cost of capital cost for profitability. “In making risk decisions we are very conscious of the customer we want to serve. Our aim is for a greater share of the customer wallet and a better understanding of the customer for the development of a long-term profitable relationship.”

Business intelligence has to be fleet and effective and capable of supporting new marketing campaigns. When the BICC asked business areas what they didn’t like the common response centred around speed of access.

“For the first time we invited all the parties into the room at the same time – Teradata, SAS, IT and the business users and we brainstormed over what we could do about the problem.” In-database processing was the solution they agreed on. Allsop-Kenney said implementing it has been difficult because so many parties were involved, but in terms of technology it has been groundbreaking and has led to a more streamlined approach. SAS and Teradata were moving into live deployment while she was in San Diego with the first set of models going through the process. The bank uploads the data automatically; the data set is created in the database.

“There is no handover, so it runs faster and you have taken out points of failure because you don’t have to move your data around the organisation.” **BT**

## Stopping the rogues

The nefarious rogue trading activities of Kweku Adoboli have cost UBS \$2.3 billion so far and brought to mind the actions of previous rogues such as Jérôme Kerviel at Société Générale and Nick Leeson at Barings. How to prevent repeat occurrences was much discussed at Sibos 2011 and subsequently, finds **Neil Ainger**.

Just why did the internal access control and monitoring systems at UBS fail to spot Kweku Adoboli's rogue trading activities? If they did spot them why were they ignored? Who was looking at the cash position, if anyone? And is it wise to allow people to move from the back and middle office to front of house trading positions? *Banking Technology* gathered a number of responses from risk system vendors and others at the Sibos 2011 show in Toronto, Canada, and subsequently, asking what lessons can be learnt for the future and investigating if better technology and Human Resources procedures might be the answer to stopping rogue trading in its tracks ...

**Phil Cantor, senior product manager, SmartStream Technologies**, said the UBS incident was "a failure of learning". The incident mirrored that at Société Générale, when Jérôme Kerviel lost €4.9 billion in 2008 by exactly the same means – namely, booking fake hedging positions into the bank system to hide his losses. He did it on a Delta One trading desk too, which typically buys a collection of shares that track an index or a commodity, metals for example, and then covers its exposure by hedging. The tiny differences in price (the delta) can lead to big profits in high volume synthetic trading but equally big losses are certain if the derivative hedging is either defective or false, as in this case. Both traders were, coincidentally, 31 years old at the time of their apprehension, although UBS' Adoboli was dealing in more recent Exchange Traded Fund instruments, particularly covering foreign exchange movements (see *news page 4 for more*).

To prevent rogue trading, as much as that is ever possible with human beings, you need a bank-wide view, believes Cantor. "Somewhere in UBS' systems were some trades that didn't add up, but the problem is finding them, raising a red flag and then acting upon it. To do this, and ensure good crisis management, you must have real-time data at your fingertips and Profit & Loss information that gives you a true balance sheet." Flexibility is key as well because financial institutions have to be able to respond to new and developing challenges.

**Jennifer Hanes, executive vice-president, reconciliations, SunGard Ambit corporate banking**, said the rogue trading at UBS represented "a failure of both systems and procedures". For UBS, or indeed any organisation, the fundamental challenge in guarding against fraud is to ask yourself what patterns are occurring in the market right now and to be constantly on the lookout for anything out of the ordinary. "Trending and analysis software can help deliver the policy and assist managers in maintaining effective oversight," she said.

"Nothing is ever static, so constant vigilance and flexible people and software are essential. In my opinion the risk of fraud is so significant – both monetarily and in terms of reputational damage – that it is worth making the investment in effective solutions and staff."

**John Groetch, business development manager at Calypso** disagreed, saying that the UBS case was neither a failure of systems or procedure. "It is a policy issue. Almost all rogue trading occurs when people from the back or middle office move into the front office. If banks implemented a policy prohibiting this move, we could have avoided the situations at SocGen, Barings, NatWest, Sumitomo and UBS. This situation doesn't require more regulation, just a change in HR policy."

Multiple layers of technology checks and balances need to be overlaid with a strong information security and access/control policy to prevent cases like this, said **Erik Stein, a vice-president and product manager for financial crime risk management solutions, at Fiserv**. A peer group analysis can also contribute towards strong oversight so that anomalies can be spotted more quickly, leading to faster investigation.

**Chris Davis, co-founder of Two Four**, said he was shocked: "You'd think the systems would have checks and balances built in, and if not, that's all the more reason to buy a system which has been vetted by other people." Spoken like a vendor of course, but he does have a point and was speaking before UBS admitted it did get a warning signal that was ignored. Like other risk experts, he

said UBS was probably using in-house systems at the time of Adoboli's rogue trades.

Davis' advice to risk managers? Test the systems and make sure they don't have holes. "Start with trade capture. When the trade comes in, make sure it is recorded. Make sure you have a confirmation from the counterparty, run the trade through the life cycle and check and vet the processes."

One of the problems, especially for the larger financial institutions, is that they have so many disparate systems, and those systems don't necessarily communicate with each other. System A sends 1,000 trades to system B, but does system B receive all of them?

Banks should focus on operational controls, said **Grace O'Donnell, deputy chief executive at Information Mosaic**. "You need wide, end-to-end control systems, which is why we offer dual or even triple verification solutions for transactions. Nothing moves until it is signed off; that needs to be part of a trading system [though of course it cannot lead to undue delays]."

Mandates limiting the amount that can be traded overall or in any one particular stock, currency or geography may also be able to help. "Our systems can categorise the types of risk facing firms and present the information in dashboards or automated alerts, which can be sent to mobile devices if a problem is detected."

But O'Donnell warns: "It can be tough to find fraud." Her company's system can look at exposure to a particular client, however, and that may have revealed problems like those at UBS, she added.

**David Gibson, director of technical marketing and strategic accounts at the data governance specialist Varonis**, says the UBS rogue trader fiasco appears to be a classic case of an employee exceeding his authority. "The bad news is that many such breaches of authorisation are never even recorded or publicised."

This case is interesting because of the lessons it can teach us about security authorisation and the need for automated alerts, he added. "You should have employee software that looks for any unusual or unauthorised patterns



and new legislation may emerge. Perhaps there might be an EU-wide regulation on rogue trading [if the industry doesn't put its house in order]," he warns.

Adoboli was likely to have been acutely aware of UBS' internal processes according to **Jane Peters, head of operations at Avertis Risk Solutions**. "Anyone motivated either for personal gain or to cover up their own mistakes, who had followed his career path of moving from the back office processing department onto the trading floor, would have the necessary knowledge to circumnavigate the safeguards and controls put in place if they are not robust enough at the outset. Risk controls need to be proactively tested and reviewed on a regular basis - including alert responses - to prevent procedures becoming too well known and too easily avoided."

"From Nick Leeson's acts at Barings Bank through to those of John Rusnak at Allfirst Financial and Jérôme Kerviel at Société Générale, whatever the motivations of rogue traders the problem has been made possible thanks to inadequate systems that allowed them to book false trades and conceal their activities; the culture within financial institutions should encourage stricter controls and oversight.

"Companies should ask themselves, would their staff be inclined to defer to a manager if they were asked to book an unusual trade or overwrite a valuation? Are their employees actively encouraged to report errors?" This might at least lessen the threat from genuine mistakes or so-called 'fat finger' incidents, if not from rogue trading itself. This kind of openness does, however, go against the macho culture of traders so this is perhaps wishful thinking.

"In our view group operational divisions need to have a much greater influence at board level in order to encourage cultural change," adds Peters. "Investment banks will continue to suffer the indignity of these headlines unless they focus on better governance."

The departure of Oswald Gruebel, the chief executive of UBS, who resigned on 24 September after the full extent of Adoboli's nefarious activities became clear, could perhaps still be in his job now if some of the suggestions above had been acted upon earlier. **BT**

of behaviour when it comes to handling organisational data or breaching the grounds of normal trading behaviour." A nebulous concept of course, as traders often pursue their own esoteric strategies. At least with automated algo trading systems breaches of the pre-programmed actions will be highlighted, which isn't to say that the original parameters programmed in at the beginning are sound either or that anyone will take notice. Trading is inherently a risky business.

That is certainly something that **Dave Excell, chief executive at Featurespace**, which provides behaviour profile software and has a long history in the gambling industry, understands. "Bets on a sporting event are comparable to trades placed on a financial market," he says. "Traders are taking risks on a minute-by-minute basis, just like the professional poker players that we track. Our software can pick up on anomalies, even if the trader is trying to mask his or her activities by using multiple pseudonyms."

The vendor's technology can be used on an individual account level to highlight problems such as when an employee is stuck in a 'chase' scenario trying to recover losses or it can identify when new aliases have been created or taken over to hide positions. If such systems can be transposed into the investment banking arena it could obviously be

helpful and Excell thinks it is feasible. "A profile of an individual can typically be established after 10 transactions. From this point on the accuracy and certainty of the modelling software improves and transactions that do not match past behaviours can be identified [and a red flag raised]."

Historical data has to be used to build the initial modelling software, however, and it can take time for the solution to mirror current trading behaviour during the early stages of an installation. Having said that, there are few other industries that can predict behaviour as well as the gambling sector so some valuable lessons could be on offer here in the fight against rogue traders like UBS' Kweku Adoboli. "The banking industry could also use some regulations in this area or a centralised anomaly reporting system," adds Excell.

**Frédéric Boulter, head of anti-money laundering and compliance at Nice Actimize**, and an ex-HSBC banker himself, backed this viewpoint pointing out that rogue traders are never charged with rogue trading as such. Prosecutions relating to false accounting and fraud are much more likely to occur, as has happened with UBS' Adoboli who was charged with these two offences on 22 September at the City of London Magistrates Court. "Rogue trading is left to the courts at the moment but in future it could become a major regulatory area



# Straight to the point

Sherree DeCovny

The unique format of the Finovate events gives a concise view of where technology is heading.

**If you have never been to Finovate in London or New York, you should go.** Produced by Online Financial Innovations, vendors have just seven minutes to demonstrate their product. At the end of the allotted period, the gong sounds and the microphone is turned off. Presentations are short, sweet and to the point. After two days, the audience comes away with a good understanding of the new technologies hitting the market, and they even get to vote for their favourite products.

More than 60 companies demonstrated their technologies at New York's FinovateFall last month. Their products fell into several categories including money management, security, social investing, online and mobile payments, and online and small business banking.

Among the Best of Show awards was eToro for its Copy.Me application, an individual and personalised one-stop e-store. The application allows expert traders, known as gurus, to generate a second line of income by creating their own investment business and showcasing their investment skills. Expert traders can create their own investment shop and start promoting their financial services to potential investors worldwide through the eToro social trading network. Copy.Me is integrated with eToro's OpenBook, which exposes gurus' trading skills to over 1.75 million registered eToro users.

T8 Webware chief executive Wade Arnold and product manager Ben Metz demonstrated Grip, a financial aggregation application that banks and credit unions of any size can use to offer mobile banking. Grip streams balance and transaction data from multiple financial institutions, displays account information and sends alerts so users have a holistic view of their finances. For example, a consumer can get information about a specific transaction they did at one Starbucks location or all their transactions across all Starbucks locations.

Financial institutions can access an analytics dashboard to see aggregate level information about the usage of Grip. This includes frequency of use, unique users over time, signature debit usage trends and heat maps of ATM locations. They can brand Grip with their own

identity. No core integration is necessary. There are no upfront or annual fees – Grip costs \$0.99 a month per active user – nor is there a minimum user agreement.

Angus Davis, chief executive of Swipely, explained how his company helps local merchants understand and engage their customers, and grow their revenue through paid loyalty programmes. Consumers earn points at particular merchants, and the rewards are automatically loaded onto their credit or debit card for use at their next visit to the merchant's establishment. Consumers can access a network of local merchants where they can earn rewards. They can check the loyalty points they have earned at specific merchants and earn rewards faster when they tell their friends about a particular merchant on Facebook. Merchants can estimate the lifetime revenue that people will drive and year-to-year customer retention. They also can understand what their customers are spending in their local community.

Swipely launched a service in Rhode Island last March, and now it is expanding into Boston, San Francisco and New York.

"Since launching the service in March of this year, we're already seeing some great traction," said Davis. "We have over 500 merchant locations running their loyalty program on Swipely today."

Jeff Chen, vice president, business development, at mShift, and Ileen Pinhasi, product manager at ACI Worldwide, demonstrated Enterprise Banker for tablet devices. Through role-play, they showed how a small business owner on the road could use the device to approve a payment to a vendor in China.

"Push notifications allow me to be aware of my company's banking activities that require my attention even when I'm doing something else," said Pinhasi. "Enterprise Banker is integrated across all points of access. So whether it's tablet, desktop or mobile, the user only has to manage one set of credentials for all different points of access."

In the demo, the small business owner logged in and was taken directly to the wireless page. The payment waiting to be released was shown on the top of the screen, and the full functionality available online was shown in a menu on the left side of the screen. Prior to releasing

the payment, the small business owner viewed a graphic display of her accounts to ensure she would have sufficient funds to make the payment. Then she transferred funds between her accounts.

The product will initially be available on iPad and Android, but it is designed to scale across other tablet platforms.

Mitek Systems's Drew Hyatt, senior vice president, sales and business development, and Diane Morgan, director demonstrated Mobile Photo Bill Pay. This application allows consumers to save money by transferring their balances on credit cards, and it allows banks to acquire new customers when they are actively shopping for a new credit card.

"The bank benefits from a much lower cost per contact, which also gets higher response and conversion rates, lowering the cost of acquisition by up to 25%," said Morgan.

The product was demonstrated on an Android, but it also can be deployed on an iPhone or a Blackberry device.

An existing customer selects "Transfer Credit Card Balance" from menu of options, logs in with secure authentication, and peruses the credit card offer. The customer is prompted to take a picture of the coupon. Mitek technology captures the 3-D image, converts it to a 2-D computer readable file and parses the information into the credit card issuer. A current APR and current account balance capture is made, and the necessary data fields are dynamically tracked to present a competitive offer.

In real time, the credit card issuer can use credit scoring methodologies and algorithms or existing pre-screening tools to present a balance transfer offer to the customer. The offer is presented. The customer accepts the offer with all the details outlined of their savings and transfers. They view the terms and conditions, accept them, and the transfer is made.

"It's just that simple. Point, shoot, transfer and save. Secure, convenient, fast and all down to my smartphone," said Morgan.

Finovate's format is truly refreshing and fun. The audience is exposed to some pretty cool applications – the above is just a small sample – and it is a great opportunity to network with banks and vendors. Thumbs up. **BT**