kx | it's about time

# Using Behaviour Analysis to Reduce Financial Crime

## Using Behaviour Analysis to Reduce Financial Crime

If gangster movies are anything to go by, taking the advice to "act naturally" would seem the best way to avoid detection before committing a crime. In police and psychological dramas, it would seem the same advice helps to avoid detection afterward too. In both cases, it suggests that a criminal's conduct, before and after a misdemeanour, can be as important in its detection, investigation and conviction as the criminal act itself. It's a lesson banks need to start learning.

For too long banks have been concentrating on the act alone, operating on the basis of fixed rules and alerts that might capture known violations initially, but fail miserably as they evolve. Moreover, by focusing on transactional activity alone, they lack context and are limited in scope. The upshot has been criminals deftly circumventing the rules while supervisory and investigation teams are weighed down pursuing false positives from poorly calibrated systems that provide no value, yet incur significant cost. Ironically, persisting with that blinkered approach is, in itself, becoming criminal as regulators demand a broader view across the enterprise and the law comes down more heavily on those who fail to provide it - as evidenced by some impressive banking CVs languishing in prison cells from Scandinavia to Singapore and from the UK to the US. So what changes are required?

Behaviours before and after a crime can be as revealing of criminal intent as the act itself and are of critical value in its detection, investigation and conviction. Focussing on transactional activity alone limits scope and lacks context.

## Rethinking Means, Motivation and Opportunity

In traditional law enforcement, the principles of "means, motivation and opportunity" are still diligently applied as the basis for proving guilt and as guidelines for deterring, if not anticipating crime. The application of these principles in financial surveillance has been somewhat less rigorous; focusing mainly on the first, making assumptions about the second, and underestimating changes in the third.

**Start with opportunity.** The traditional approach to containing opportunity, and one accelerated in the wake of early cases like Nick Leeson in Barings, has been in areas like segregation of duties, multiple levels of workflow and enforced desk leave. But all are throwbacks to a physical age when the back office was sacrosanct, the concept of outsourcing was anathema and presence was physical. Pitch forward to today with distributed, cloud-based and possibly shared-processing facilities, all with remote access, and it's clear that while they still make sense, they need modernising. Opportunity threat has quickly become much more complicated and can be exploited at levels beyond proximity and presence as the free flow of information, porus chinese walls, overlapping connections and instantaneous communication offers possibilities previously unconsidered. Opportunity need no longer remain local and isolated, it can be distributed and collaborative.

**Motivation is changing too.** While few of the most notorious rogue traders may have made personal gain from their violations (they were driven mainly by ego and attempts to cover up previous mistakes) the same is not true of those engaged in money laundering, insider trading and other collusions so prevalent today.

Banks need to extend their detection beyond static alerts alone and look to behaviour analysis as a means of identifying conduct risk

For them, that is their prime motivation. More insidiously, however, in an age challenged by extremes of anti-capitalism and terrorism, it may, for others be as much about wealth destruction and societal disruption as about personal gain. Such motivations often lead to less targeted crimes, ones whose randomness and speculative nature make them more difficult to discern than those of focussed intent.

It represents the incursion of cybercrime into financial crime, based on the hijacking of transaction systems as opposed to their misuse. Even worse, the culprits may not be your clients, let alone your staff; they may simply be anonymous actors whose goal is less about making gain and more about causing pain. In short, motivation, and dealing with it, has become a lot more complicated.

**And that leads to the means.** Banking has typically considered the means as the transactions that appear to consummate the crime; the trade that exceeded the limit, the series of trades the moved the market or the close-out that realised the seemingly undue profit. Yet alerts on each transaction may, after exhaustive and expensive investigation, point simply to a delayed cancel order that cleared the limit, a sequence of above-board client orders that were executed honourably or what transpired to be a serendipitous trade just before a favourable news announcement. Meanwhile, someone else is busily conversing with a former colleague on chat, carefully sequencing trades to escape limit checks and checking emails from a back-office contact on what codewords to enter to bypass internal settlement checks. That's where the ill-intent may be revealed. Yes, some alerts, like spoofing or layering, may look across a set of transactions, but they do not look at the more subtle behavioural aspects that underlie them, or the other tools and channels (i.e. means) being used as part of the subterfuge.

## Detect and Deter: The Value of Behaviour Analysis

So, across all three is the recurrent theme that it's not just the transactions that need to be monitored, it's the behavioural activity around them as well. Using behaviour analysis, the prevalence of a specific term, the uncharacteristic frequency of an action or set of actions, or the connection and communication profiles to third parties may reveal indications of criminal intent. Equally importantly, the knowledge that such behaviour analysis is in place may discourage many more. Conduct risk must be both monitored and known to be monitored; the former to detect, the latter to deter.

Not only does behaviour analysis improve detection and investigation of financial crime, it acts as a deterrent that further reduces risk and cost

Behaviour analysis can range from relatively simple comparisons against personal, peer or industry benchmarks to NLP investigation of eComms data and correlation with outside events.

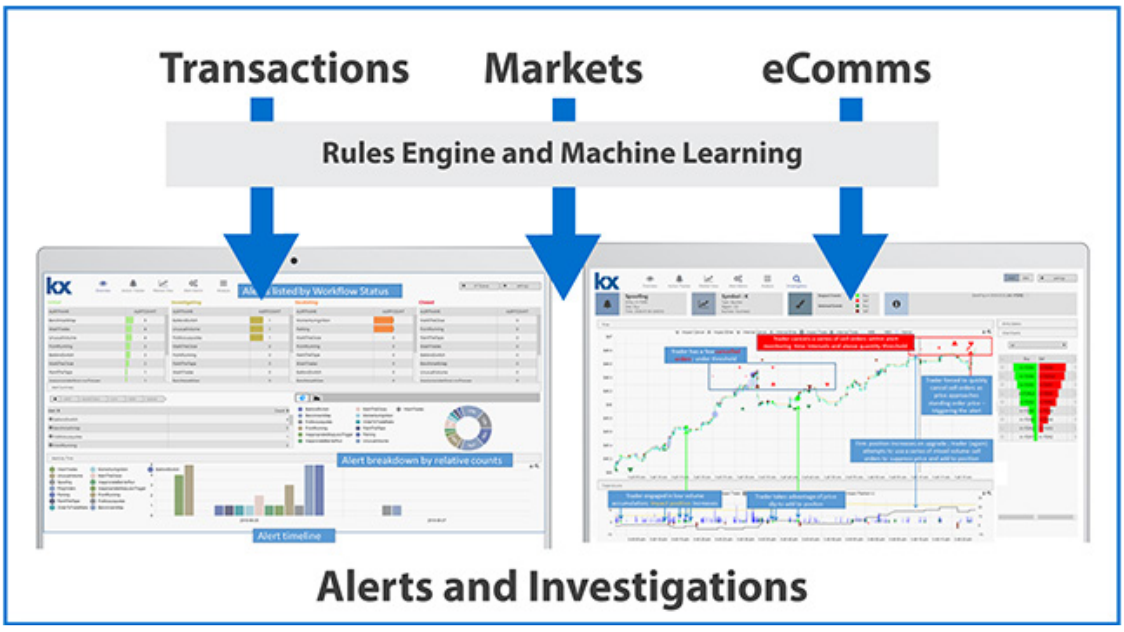
Behaviour analysis can range from relatively simple comparisons against benchmarks to advanced techniques like natural language processing (NLP) trawling through eComms data for the predominance of a particular phrase, its correlation with outside events and possibly linkages between parties involved.

At one level, "act naturally" is already the principle behind some traditional alerts for detecting large orders, unusual volumes or high cancel and amend rates where activities are measured against the norms of the individual, their peer groups or other benchmarks and excess deviations are flagged.

Indeed, such an approach is advised in the **ESA's compliance and reporting guidelines**, and beyond the transaction level it may track numbers like the frequency of emails, the duration of phone calls or the concentration of recipients. But, while providing some insight, each in itself is simply an isolated alert and suffering the same limitation as transaction-only alerts – lacking context.

## A Client Example

Of greater value, therefore, would be analysing the content of the communications to look for suspicious terms, changes in language or correlating the message directions with transaction instructions to detect possible linkages. This was the driver behind one of our clients who wanted to analyze unstructured data in emails, instant messaging and voice transcripts by using flexibly defined lexicons (effectively metadata on words and phrases) to raise alerts based on configurable rule sets using NLP.




**Behaviour Analysis over Consolidated Data**

At a system level, such processing relied on the ability to extract, load and lemmatize unstructured data from multiple sources before applying NLP analysis. Using Kx for Surveillance as the platform for all its data ingestion, trade monitoring and alerts management enabled the client to interleave transactional data including trades, orders, quotes and market data, with trader communications including email, chat and call transcripts.

This combination allowed it to correlate eComms behavioural data and metadata with transactional data for more informed contextual investigations into suspected trader misconduct. Integrated dashboards for alert management and workflow coupled with search and retrieval capabilities for direct access to the original data (eg: images, voice) further improved the speed and productivity in investigating, tracking and closing-out investigations. The solution provided a compelling illustration of the benefits of consolidated surveillance data as discussed in **our previous paper.**

## Effective Surveillance: A Process, not a Project

Notwithstanding its undoubted power and potential, behaviour analysis should not be viewed as a turn-key panacea that instantly addresses all the short-comings of rules-based analysis. As with all machine learning, the secret is in that second word, "learning", in recognising the importance of data and continually retraining the underlying models. An out-of-the-box solution will not, for example, be able to preemptively detect a first-time use of codewords between colluding parties as proxies for communicating stock names and indicators of their upcoming financial results. That possibility may be surmised by humans but the exhaustive checking and validation can best be done by that first word, machine.

Implementing behaviour analysis is an iterative process where past improvements can be factored into new analyses via machine learning and Natural Language Processing techniques - so early adoption can deliver early benefits.

Then, if the results are fed back into the model, they may not only confirm the original hypothesis but may also, in having access to consolidated historical data, detect similar previously unknown examples that may inform the investigation and support the current conviction. It's part of the virtuous circle of improving model accuracy and reducing model drift that makes machine learning so powerful.

Such iteration illustrates a core difference between effective surveillance and standard banking initiatives. It does not have the comforting bookends of "As Is" and "To Be" states and a well-defined project plan to bridge them. The end point is unknown and unknowable. Effective surveillance is a combination of defence and offence, catch-up and leapfrog. It is a process, not a project.

## ♪♪ And all I gotta do is, act naturally ♪♪ [1]

In theory, effective deterrence should not just reduce the frequency of detection, it should obviate the need for it. In practice, however, low levels of detection may just as accurately indicate its poor quality and cessation may, in any event, be temporary. So, as with standard law enforcement, the path to informed detection and deterrence of financial crime will be an on-going and evolving combination of humans and machines that will be discussed in a follow-up paper in this series.

In the meantime, and back to the movies, if a film is ever made about trading and market surveillance it has to be hoped that the mood music in the soundtrack would progress from ♪♪ Act Naturally♪♪ at the outset to the more sublime ♪♪Ain't misbehavin'♪♪ at the end. That way, institutions, careers and indeed ears, may be better protected.

[1] *By the aptly named "Buck Owens and the Buckaroos"!*

## About Kx

Kx has been at the forefront of data driven solutions for the last 25 years. The core technology, specifically built to analyze and identify behavioural patterns across huge volumes of real time and retrospective data is used by every Tier 1 Bank in the world. The unique combination of leading edge technology and a large body of technical and capital markets expertise, makes Kx the right partner to deliver a strategic consolidated platform for both current and future regulatory obligations together with continuous improvements in risk-based profiling and productivity.

Surveillance and regulatory clients include banks, regulators, exchanges, brokers, proprietary trading houses and investment firms globally.

# Kx Solutions

## Kx for Surveillance

Kx for Surveillance is the world's first integrated platform for consolidated multi-factorial detection and investigation of market abuse, financial crime and fraud. Delivered with a complete library of MAR, eComms and AML models, new models can be added and easily incorporated into the comprehensive alert, workflow and case management infrastructure with full contextualized, granular-level investigation tools.

## Kx Data Refinery

Kx Data Refinery provides a complete suite of tools for managing data from ingestion through to consumption by multiple parties in a consistent and controlled manner. Built on Kx technology, our solution combines the speed and performance kdb+ with powerful analytics and the rich visualization of Kx Dashboards.

## Kx for Flow

Kx for Flow is a HTML5 white label foreign exchange trading platform offering users the ability to create bespoke liquidity pools and distribute price information to clients and markets. Our comprehensive turn-key solution provides in-depth risk management functions as well as real-time in-memory analytics.

For a discussion on how Kx could help your specific requirements, please contact **sales@kx.com**

**Head Office**
3 Canal Quay,
Newry,
BT35 6BP
N. Ireland
Tel: +44 (0)28 3025 2242

**Belfast**
The Weaving Works
Ormeau Avenue
Co Antrim
BT2 8HD, N. Ireland
Tel: +44 (0)28 9023 3518

**Dublin**
6th Floor, Block A,
1 George's Quay Plaza,
Dublin 2, D02 Y098
Rep. of Ireland
Tel: +353 (0)1 630 7700

**London**
5th Floor,
Cannon Green Building,
27 Bush Lane,
EC4R 0AN, United Kingdom
Tel: +44 (0)207 337 1210

**New York**
45 Broadway,
New York,
NY 10006
USA
Tel:+1 (212) 447 6700

**San Francisco**
535 Mission St,
14th Floor
San Francisco, CA 94105
USA

**Toronto**
31 Lakeshore Road East
Suite 201
Mississauga, Ontario
L5G 4V5 Canada
Tel: +1 (289) 329 0636

**Ottawa**
300 Terry Fox Drive,
Kanata, On,
K2K 0E3
Canada
Tel: + 1 (613) 216 9095

**Sydney**
22 Pitt Street,
Sydney,
NSW 2000
Australia
Tel: +61 (0) 2 9236 5700

**Singapore**
One Raffles Quay,
North Tower #30-03,
Singapore
048583
Tel: +65 6592 1960

**Hong Kong**
Level 66, The Center,
99 Queens Road,
Central
Hong Kong
Tel: +852 3965 3181

**Tokyo**
20F Shin-Marunouchi
Center Building,
1-6-2 Marunouchi,
Chiyoda-ku, Tokyo,
Japan 100-0005
Tel: +81 (0)3-6634-9799