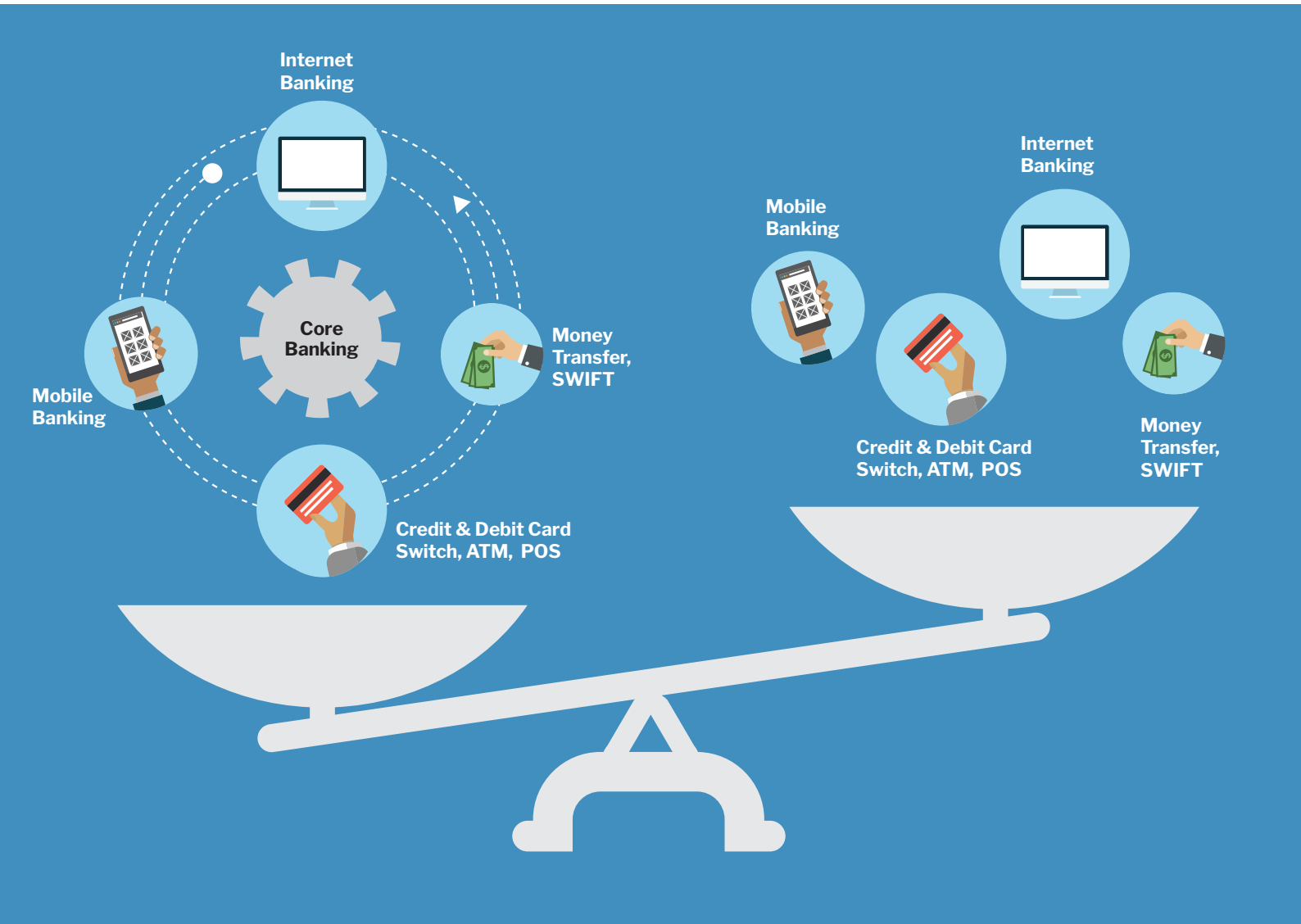
WHITE PAPER

Clari5 by CustomerXPs®

Break Filter Bubbles in Banking Enterprise Fraud Management

Synthesize Holistic Wisdom From Core Systems and Not Just From Channel Silos!



WHITE PAPER

Clari5™ by CustomerXPs®

Break Filter Bubbles in Banking Enterprise Fraud Management

Synthesize Holistic Wisdom From Core Systems and Not Just From Channel Silos!

A Core Banking-led Enterprise Fraud Detection System provides five distinct advantages over silo-ed Delivery Channel based systems; namely the depth of analysis, ease of configuration and implementation, cross channel fraud detection, insider fraud detection and a real time highly available fraud detection engine by default rather than as an add-on feature. This paper explores these key differentiating aspects further.

Clari5™ by CustomerXPs®

The Deep Sea

Core banking system is where 80% of the data will be available for fraud intelligence including customers, accounts, employees, all channel financial transactions, remittances etc.

Use of key information available for customer/account in conjunction with the alternate delivery channel transactions is key in effective fraud detection.

"Over 60% of our planet is covered by water more than a mile deep. The deep sea is the largest habitat on earth and is largely unexplored. More people have traveled into space than have traveled to the deep ocean realm...."

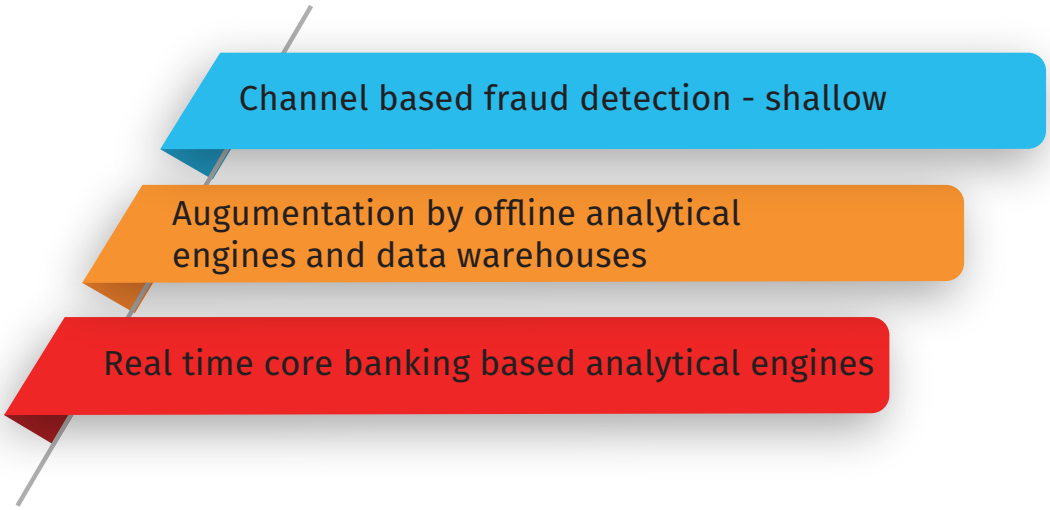
- The Blue Planet Seas of Life

Most of the customer experience analytics and fraud analytics data obtained from the point of sale or point of interface with the customer, for example, from the POS machine, the browser the customer uses or the mobile app the customer uses, provides a certain kind of analytics, and customer behavior information.

Such analytics is quite well analyzed and understood to the point of being commoditized by the major data analytics players. For example Twitter sentiment analysis can be setup on Azure with just a few clicks, in under 30 minutes.

However, the information and insights that such analytics provides is limited in usefulness, because there is more marine life "a mile deep in the sea" which is yet unexplored.

Getting more insight into customer behavior and detecting fraudulent patterns requires a more advanced, state-of-the-art product thinking, where the organization's brain and memory locations are tapped till the depth of the ocean floor.



As an example, a new mobile app user could get their rent payment flagged owing to it being the first transaction via the app, whereas a core banking system already has the information that such a recurring payment has been happening since the past 12 months.

So a false positive may be generated because there is no way to offset it with existing information about the account's history which is stored deep in the financial institution's brain.

Another example where a true positive may be missed is when amounts below the threshold are being debited fraudulently via internet banking, but they are not being correlated with the history of the account's transactional behavior, which does not have such recurring micro payments. An unusual pattern, which when conducted at a large scale across multiple accounts can lead to even larger fraud values.

Again, missing the correlation of these payments with the absence of such payments in the past, across multiple accounts, and benefitting a particular fraudster, will lead to an undetected fraud or delayed detection of fraud.

Clari5™ by CustomerXPs®

The Chicken's Neck

Fraud risk assessed for an internet banking login initiated from a new device for the customer vis-a-vis fraud risk assessed for an internet login initiated from a new device for the user who is senior citizen and that underlying account has not seen any transactions in the last 90 days (near dormant).

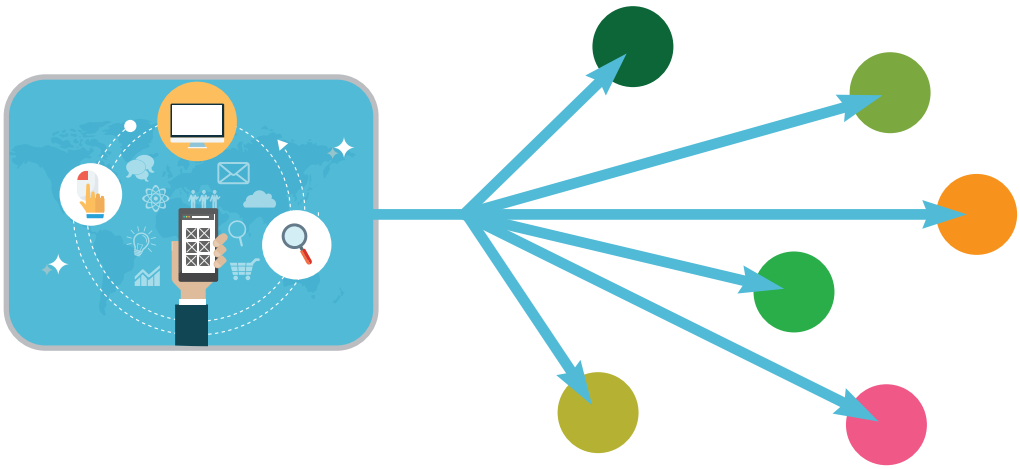
The shortest sea path from Asia to Europe, since 1869, has been via the Suez Canal. The Suez Crisis of 1956 indicates how critical the Canal had become; simply monitoring and taxing the traffic into the Canal led to political and financial gains that were disproportionate to the actual military strength of the parties involved.

There are other examples in geography and medicine related to the chicken's neck, for example, Siliguri being the only land connection between India's northeast and the rest of the country, or the carotid artery in the human body, that are critical for an entity's survival.

The core banking system based fraud detection and prevention systems act like a chicken's neck (or the fraudster's neck in this case) because all financial transactions - movement of money, as well as non-financial events that can lead to a financial transaction - must pass through the core banking system.

The business analyst has the tools to identify which particular channel was used to initiate a financial transaction and therefore channel specific rules may also be configured, however, many a times, very simple business rule configurations that apply across multiple channels can be levied at the central core of the system, leading to a very secure and robust fraud detection engine.

Another advantage of this approach is that there is no need for redeployment or re-implementation whenever new channels are added as layers above the core banking system. The fraud detection is already in place, and it can be tweaked if needed with channel specific rules.



A Rose By Another Name

Fraud Risk assessed for internet banking funds transfer transaction vis-à-vis fraud risk assessed for internet banking funds transfer transaction for an account which has seen a sudden surge of credits recently into the account through multiple modes, e.g. Mule/ponzi accounts.

"You can fool some of the people some of the time, but you can't fool all of the people all the time."

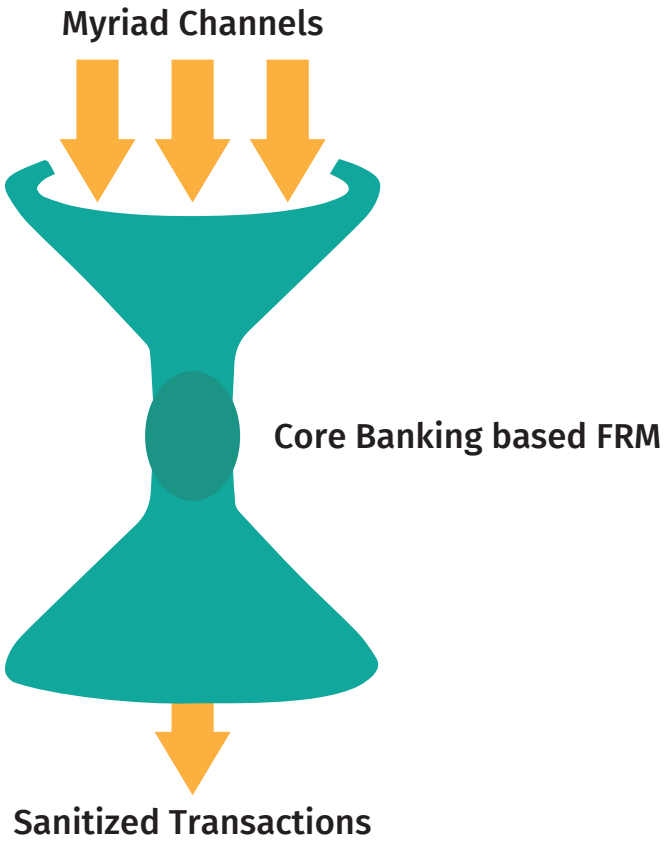
- Abraham Lincoln

The fraudster - fraud detector is a cat and mouse game, with each party trying to get the better of the other with their respective next moves. Channel level limits are very common to detect and circumvent, for example, an internet banking system may not allow a payment until 30 minutes after registering the payee. The value of 30 minutes is known. Similarly, after multiple attempts, transaction velocity related limits per channel can also be found easily by fraudsters.

The next step after obtain this intelligence is to use all the available channels at the disposal to architect a well-thought-of multi-channel fraud that flies under the radar of the individual channel sniffing, shallow fraud detection tools.

This is where a core banking based fraud detection system kicks in. It can detect the rose - or the absence of it - at the point when a fraudulent debit is made, because of the history and profile built for all the parties involved, be it the employee, the customer, the device, the channel being used.

All this combined gives a unified view to the fraud detection team, and that is a luxury not available to the snipers sitting at the borders, tracking the passage of information via one individual channel.



The Houdini Inside

Insider fraud attempts and employee colluded fraud attempts cannot be detected with alternate delivery channel approach only. For e.g. employee doing multiple balance enquiries on near dormant account and subsequently internet banking account take over attempts for one of those accounts

"Relevant internal controls, including independent risk management, have to be established for all business activities."

- Barings Bank Investigation

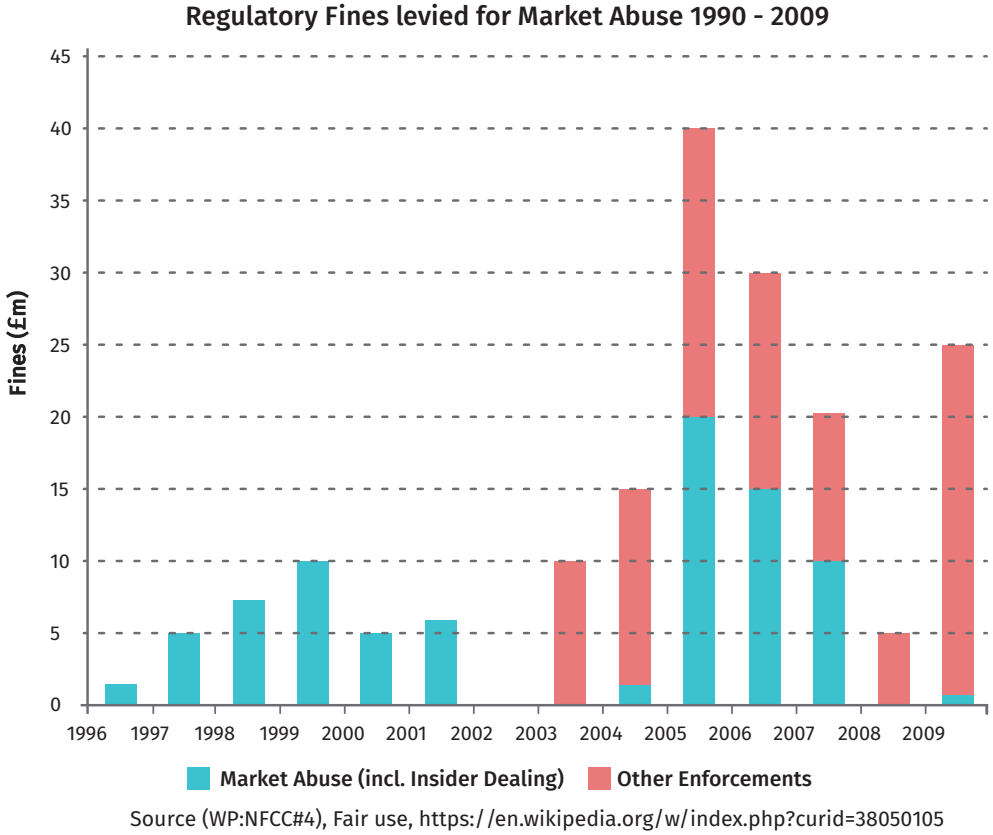
How does one detect the Houdini inside? One Nick Leeson can bring about the fall of a 200+ year old Barings Bank. The risks of not being able to detect non-channel fraud are just not worth it.

A core banking based system can help the financial institution keep track of which operations were performed when on the bank's internal systems, right from complex financial transactions to simple login and logout events in off hours, or multiple account inquiries on specific accounts over a period of time.

Such events can get the needle of suspicion pointing in the right direction well before the intent to defraud becomes an actual fraud.

Secondly, employees being questioned and warned for suspicious activities keeps from converting potential fraudsters out of fear of being found out.

It is practically impossible for the channel based fraud detection tools to replicate this level of depth in fraud detection. A core banking based solution sitting right at the point of financial transaction commit makes specialized knowledge of internal processes a useless weapon when a rogue employee attempts to commit fraud.



Source (WP:NFCC#4), Fair use, https://en.wikipedia.org/w/index.php?curid=38050105

Clari5™ by CustomerXPs®

Real-time, All the Time

Complex fraud schemes like advance fee fraud/lottery fraud and remittances fraud involve usage of multiple channels including branch transactions, inward remittances, internet banking funds transactions, ATM withdrawals. Detection of these kind of fraud schemes will be lot more effective only if core banking monitoring is also done.

A system fit for fraud risk management solution for alternative delivery channels only may not fit for enterprise wide fraud risk management & real-time monitoring for core banking. Core banking real-time fraud monitoring needs a more technically robust and scalable solution since the TPS of core banking is way higher than the TPS of alternative delivery channels.

"A creed that we all lived by: Failure is not an option."
- Gene Kranz, NASA Mission Control Center

A core banking based fraud detection solution, by the very nature of the monitoring, has to keep pace with the pace at which transaction happen. It cannot be a silo based backend engine that churns out an insight after a few months, weeks or days. Also it has to be up all the time, there is no downtime for a modern bank in the web era.

This is the reason it is challenging to build a core banking based system. While frauds must be detected, regular transactions, which are a vast majority, should clear scrutiny without any time lag. However, a fraud detection engine that is designed to work with a core banking system to begin with, will have real time analytics built in and will also have high availability built in.

For a system that starts from the peripherals, both options exist, i.e. real time vs batch mode. However when real time analytics is a constraint to begin with, core banking based fraud detection systems have real time results and high availability pre-baked into the product. It is not an add-on or additional feature, but it comes with the package right from the architecture and design stage. This provides the financial institutions a powerful fraud detection engine that is guaranteed to be highly available and real time.

Availability in %	Downtime			
	Per Year	Per Month	Per Week	Per Day
95 %	18.25 days	36 hrs	8.4 hrs	1.2 hrs
98 %	7.30 days	14.4 hrs	3.36 hrs	28.8 hrs
99 % ("two nines")	3.65 days	7.20 hrs	1.68 hrs	14.4 hrs
99.8 %	17.52 hrs	86.23 mins	20.16 hrs	2.88 mins
99.9 % ("three nines")	8.76 hrs	43.8 mins	10.1 mins	1.44 mins
99.95 %	4.38 hrs	21.56 mins	5.04 mins	43.2 sec

The advantages provided by a core banking led approach to fraud detection have been capitalized by many large and small financial institutions across the globe. Being a sensitive topic for banks, no individual case studies are provided in this publicly available document. Specific case studies and customer visits can be arranged by contacting us at clari5@customerxps.com