Fighting Theft and Fraud in Financial Services With Innovation that Matters from IBM

Financial theft and fraud have become a global, hyper-growth "industry". Targets include not only traditional retail banks, but increasingly also credit unions, wealth management, private banking, and securities firms. If you move information about money, you can't afford business as usual.

Highlights

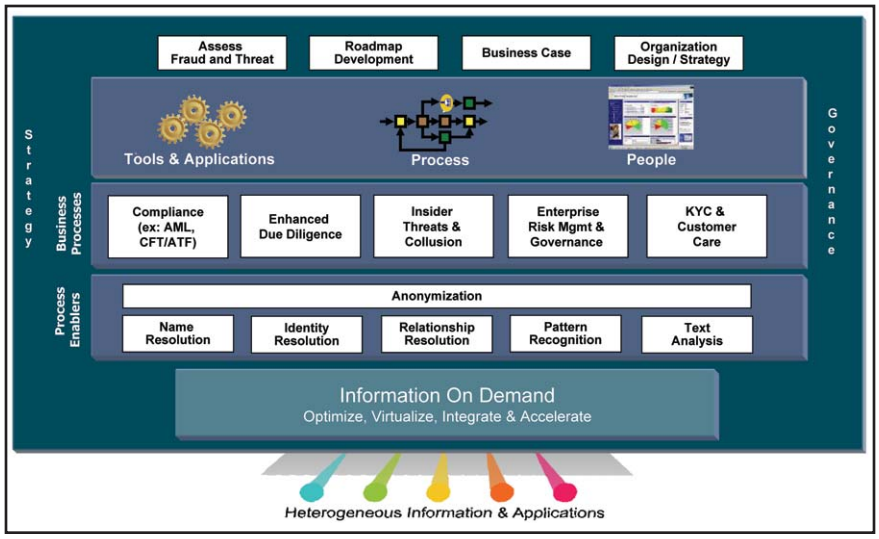
- ***Intensifying Threat, Fraud & Risk challenges are pushing financial services clients to a tipping point – they need to transform.***
- ***Fighting Threat, Fraud & Risk requires a new depth of capability in recognizing and serving customers***
- ***IBM's core strength in Information Management and our new Threat and Fraud Intelligence capabilities position IBM as the leader in this field.***
- ***This solution not only mitigates threat, fraud and risk, but can also strengthen customer relationships and enable innovation that matters.***

The Problem

Threat and fraud issues are intensifying. The frequency and types of threats are increasing dramatically. Threats are increasingly asymmetrical – that is, related in non-obvious ways making them much more difficult to detect. The perpetrators of fraud range from elderly people using minimal "technology" to criminal and terror syndicates with sophisticated global fronts and networks. Astute criminals take advantage of many cultures around the world to hide identities and assets.

Insider theft and collusion continue to cost banks millions of dollars a year, accounting for over 50% of all losses according to many different sources. Simultaneously, regulatory pressures are expanding, as well as increasing public sentiment that financial services companies should do more to protect their clients.

The common element across all forms of threat and fraud are humans. People, be they current or potential clients, employees, contractors, vendors or business partners, are both your most important asset and your biggest liability.



A global integrated repository for threat and fraud that serves as a single source of information and deep analysis into your key identity assets.

The key to mitigating threat and fraud is to stop it before it can actually take root within the system or organization, but recognizing a potential threat trying to misrepresent their identity is a difficult task.

Banks have millions of customers and hundreds of millions of customer records. They have multiple products and services, delivered in virtually every fashion. Applicants can access services from the secrecy of their own living rooms. Individuals are free to misrepresent themselves on online credit or loan applications by simply changing the way they spell their name, or by using a false or stolen identity.

Criminals can hide within the disparate systems of large banks, be it the regional database of a retail bank acquired by a Money Center bank, a CRM application that formats data in a manner that cannot be shared with the rest of the system, or an hourly customer service representative who carelessly enters the wrong account information.

> *A major national bank provided clients something better than 7-day service – one branch manager opened its doors to drug traffickers and professional money launderers and helped commit their crimes. Result: They signed a deferred prosecution agreement and forfeited $10 million to the U.S. Department of Justice for criminally violating the Bank Secrecy Act (BSA).*

Many banks employ watch list filtering and KYC procedures in their security controls but most of these systems are based on archaic name matching technologies not equipped to deal with the infinite variations of name cultures, spellings, combinations, genders titles, prefixes, nicknames, that plague these systems with false positives and negatives

Establishing a trusted "identity" involves much more than just one or more combinations of names, rather it involves deep analytics that maximize all of the banks person information assets. You must consider current and past addresses, phone numbers, government identification(s), and a variety of data points to establish a concrete identity.

Then you must make sure you understand the relationships among identities. It matters both to you and to governmental agencies if someone wanting to open an account with you (or worse yet, gain employment) has shared an address with someone who shared a mobile phone number with someone who is on a suspicious persons list.

The Solution:

Threat & Fraud Intelligence

Early adopters are beginning to recognize the need for significantly improved threat and fraud intelligence

capabilities in financial services. They know this must address all aspects of identity recognition and resolution, as well as relationships among individuals around the globe.

Working with leading-edge clients and technology providers, IBM has assembled an innovative Threat and Fraud Intelligence solution for Banks and Financial Markets - ***a global, integrated repository for threat and fraud that serves as a single source of information and deep analysis into your key identity assets***, including:

- Multi-cultural name recognition
- Real-time perpetual analysis and resolution of true identity
- Non obvious relationship linkages to detect "networks" and relationships
- Leverage your existing investments in knowledge based applications (CRM, HRMS, MDM, AML)

> *A major global banking organization found a 97% accuracy in detecting "bad guys". Plus, 127 relationships were identified that were previously unknown to the bank that prompted immediate investigation and analysis (employees related to vendors, employees who were also vendors, etc.).*

The IBM Information On Demand platform enables banks to unlock information from application and database silos across the enterprise and beyond, optimize and integrate it, and place it in the context of Threat & Fraud process enabling tools.

- Name Recognition detects and resolves multi-cultural variations of names
- Identity Resolution detects persons creating multiple identities
- Relationship Resolution detects networks of persons engaging in suspicious or illegal activities, like Anti-Terrorist Funding links

The special insight and analysis produced from these specialized tools can then be fed into the bank's key business processes, like enterprise risk management, compliance, due diligence or corporate governance applications to help detect suspicious persons, networks and activities and prevent fraud.

Improve Due Diligence - AML, Anti-Terrorist Funding

- Most existing AML systems cannot guarantee whether they are monitoring the accounts of multiple persons or a person using multiple identities
- Improve monitoring for and reporting unusual or suspicious activity
- Improve AML compliance with better understanding of names across global cultural boundaries and variations, complete identities (names, addresses, numbers), and networks

Insider Threats and Collusion

- Understand exactly who is on your internal payroll (employees and vendors) and detect linkages between employees, vendors, applicants and other third parties
- Detect and prevent losses before they occur
- Reduce revenue loss due to insider collusion by enabling better screening of employees, vendors & future applicants

Enterprise Risk Management, Compliance and Corporate Data Governance

- Lower risks by better understanding your identity assets
- Reputational and brand risk
- Operational and concentration risk
- Regulatory and legal risk
- Improve your ability to respond rapidly and thoroughly to government information requests (ex: 314(a), subpoenas, regulator requests)

Improve Customer Care and Know Your Customer

- Improve view of the client – all accounts, all channels, relationships within households, families, and any commercial accounts
- Improve compliance with KYC regulatory requirements

Conclusion

Question: Why bother fighting theft and fraud? The task seems so huge and complex, maybe the easiest thing is to do nothing and wait for the next theft.

Answer: Because winning each battle means Improving revenues and profit.

- Increase revenues, profits and operational efficiencies by significantly improving your analysis and insight into your key identity assets – your current and potential customers, employees, business partners and vendors
- Cost savings and cost avoidance in meeting regulatory compliance reporting and requirements
- Decrease risk of loss and fines. Even one major incident can be reported globally and cause dramatic loss in shareholder value and client trust.

Leading-edge bankers realize they can lower risk and therefore lower capital reserves by significantly deepening their understanding of current & potential clients, employees and vendors. This is a new wave of innovation that matters that you can't afford to miss.

A large UK bank discovered that one of their previous Bank Managers of the Year had committed fraud of over 21 Million Pounds ($38 Million USD). As a business manager, he had the authority to open personal bridging loan accounts and created new customer ID numbers using details of customer info, sometimes merely by dropping one letter from a customer name.

For more information

To learn more about IBM's Threat & Fraud Intelligence solutions for banking, please visit: **ibm.com/db2/eas** or contact your IBM sales representative.

IBM (United States of America)
Entity Analytic Solutions
6600 Bermuda Rd, Suite A
Las Vegas, Nevada
United States of America, 89119

Printed in the United States of America
6/06

G507-1486-03