IBM Analytics
White Paper

Financial Services

IBM Counter Financial Crimes Management

Gain superior clarity on identities and relationships linked to financial crime activities with entity analytics

Fraud, money laundering and other financial crimes are a thorn in the side of every financial institution. These activities can cut into profits, damage public trust and expose banks to massive regulatory penalties if found to be out of compliance with governmental regulations. Many organizations simply accept financial crime as an inevitable cost of doing business. But today, armed with advanced identity resolution and new kinds of analytics, financial institutions have powerful tools at their disposal to reduce fraud and money laundering.

The IBM® Counter Financial Crimes Management solution offers rich analytics that help banks gain a clearer view of entities, relationships and hidden patterns as they deal with financial crimes including anti–money laundering (AML), anti-terrorist financing and various types of fraud. It provides an ecosystem of analytical and investigative tools designed to work together as a single, integrated solution. By using the solution to gain deeper insights into customers, relationships and context, financial institutions are better equipped to meet regulatory requirements and prevent financial crimes before they occur.

Increased AML requirements necessitate more robust countermeasures

Today's cybercriminals are agile and technology-savvy, driving ever-more sophisticated attacks on the industry. They are also highly organized, with more than 80 percent of cybercrime acts estimated to originate from some form of organized activity.[1] Money laundering schemes frequently include both shell companies and fictitious people, and they change constantly to conceal illicit activity and assets. As a result, money laundering risks are given regular and formal attention at board meetings—and for good reason.

The frequency of money laundering schemes is on the rise. An estimated 2 to 5 percent of global GDP, or USD800 billion to USD2 trillion, is laundered each year.[2] Specific to developing and emerging economies, the impact was USD6.6 trillion in illicit financial flows from 2003 through 2012.[3]

Regulators are increasing and strengthening regulatory requirements in an effort to address the upward trend of complex financial crimes. Evidence of this sentiment may be found in the highly anticipated release of the US Treasury Department's new customer due diligence (CDD) requirements and the European Union's latest AML directive. These proposed rules are designed to enforce more rigorous CDD tracking, which will enhance financial transparency and help safeguard the financial system against illicit use. They will also include an improved regulatory requirement to identify beneficiaries of legal entities, subject to certain exemptions and enhanced due diligence (EDD) when individuals or groups are identified as qualifying for exemptions.

Compliance with these new regulations compels institutions to make more informed, insightful and consistent decisions that strengthen the effectiveness of compliance programs. Implementing these changes can be operationally and technologically burdensome. But noncompliance with AML laws carries a hefty penalty and the fines for violations of AML and CDD may be directed at either senior executives or institutions. In 2012 HSBC agreed to pay a record $1.92 billion in fines to U.S. authorities. And while in 2014 only 45 anti-money laundering (AML) infractions were issued, the penalty costs rose. Banks paid USD351 million in 2014, or roughly 7 times the fines levied in the previous year, excluding concurrent fines with fines being levied on the c-suite as well.

Understanding customer relationships is vital to fighting financial crime

Financial crimes can be complex, often spanning national borders. Combatting them involves a range of challenges, including:

- Correctly identifying a bank's "customer", whether it be an individual or organizations
- Understanding hidden patterns and relationships among customers
- Covering the cost of investigations and compliance reporting
- Reducing false positives to prevent unnecessary investigation of legitimate transactions
- Increasing detection speed to limit losses and customers' exposure

To detect suspicious activities, institutions must understand more than just their own customers—they need a clear understanding of their customers' customers as well. Unfortunately, most financial institutions currently use rule or profile-based engines that are not agile enough to adapt to today's fraud and AML's ever-changing schemes. Anticipating that newer tools and processes will be required to keep up with these changes, financial institutions also insist that any technology change must augment—not replace—the significant investments they have already made in fraud and AML systems.

The IBM Counter Financial Crimes Management solution helps banks tackle these challenges with a multilayered ecosystem of complementary analytical techniques, including crucial entity analytics capabilities.

The solution is designed to complement organizations' existing investments in anti–financial crimes technology. It helps eliminate information silos, expands the observation space and enables unified enterprise business intelligence. By using a full array of tightly woven big data, entity and predictive analytics capabilities, the solution can analyze data from both internal and external intelligence sources. This allows financial institutions to mix and match the right tools to apply to each unique fraud or financial crime scenario.

Entity and relationship analytics help banks understand customers in real time

Understanding whether the bank is working with the right person and whether each transaction is legitimate is vital throughout the entire customer lifecycle—from account opening through every deposit, transfer, investment and withdrawal. The Context Computing features within IBM Counter Financial Crimes Management leverage advanced entity analytics specifically optimized to recognize nefarious individuals and organizations in spite of sophisticated attempts to mask their identities, unscrupulous relationships and activities.

There are three vital aspects of knowing your customer:

1. **Identity resolution (who is who?):** By accumulating identity context over time, the entity analytics feature uses various enterprise sources of information to determine whether individuals really are who they say they are. Proprietary IBM Context Computing technology looks at these attributes across time to help ensure the most accurate identity and determines whether a previous assumption should be corrected based on new facts.

2. **Relationship resolution (who knows who?):** Once accurate identity is established, complex relationships can be uncovered. The system processes resolved identity data to determine whether people are—or ever have been—related in any way.

3. **Multilayered analytical processing (who does what?):** With "who is who" and "who knows who" well established, the IBM Counter Financial Crimes Management solution then applies additional layers of analytics processing to evaluate all transactional and non-transactional behavior of the entity—and optionally, of associated entities as well—to assess downstream compliance and fraud risks.

An enterprise-wide view of each customer across all lines of business and geographies is needed to clearly identify and understand the associated relationships. By establishing this comprehensive view at the start of the customer relationship, financial institutions dramatically reduce opportunities for new account fraud and increase their odds of discovering well-concealed criminal activities.

Name resolution is an important—albeit often problematic—part of these processes. There are no consistent standards for names. Some countries mandate standards, but they vary from country to country. Nicknames, transliterations between languages, multiple family names (common in many countries), different orders of names and many other factors make the variations appear very different.

In addition, personal and corporate names are often represented differently in diverse onboarding systems, or the people involved may provide conflicting information. Often, this is unintentional and the result of human error (for example, names are mistyped or misspelled), or the same person may have different roles within the same company (beneficiary in one instance, account holder in another). Intentional misrepresentation of identities, however, is typically a sign of fraud.

Build entity and relationship awareness

In isolation, no single data point is particularly useful in allowing financial institutions to understand customers—but in context, the information begins to create a comprehensive picture.

IBM Context Computing technology features look at individual data points much like jigsaw puzzle pieces. By looking for relationships between pieces, entity analytics can take a large data set and begin identifying which pieces may be related, as well as which are connected (see Figure 1). And, additional connections will be established as the bank continues to tap into other data sources from within the corporation along with various external sources and watch lists.

As more connections are made over time, the relationships become more apparent and fitting new pieces of data into the overall picture becomes easier. Each element refines the complete view, providing greater clarity and more focused insight.

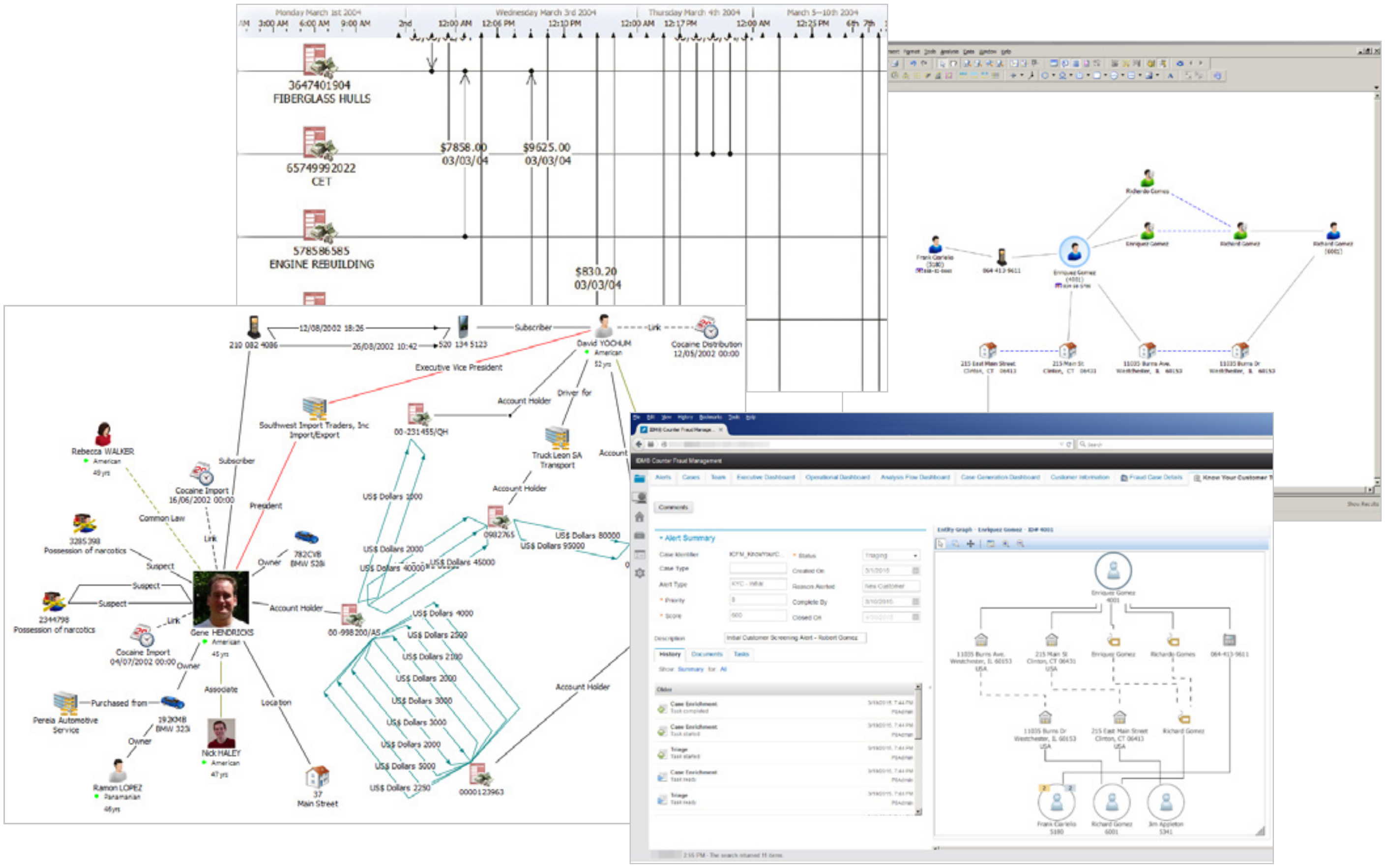

Figure 1. IBM Counter Financial Crimes Management leverages entity and forensic analysis and automated discovery to display unknown relationships for investigation.

A holistic solution that incorporates the strength of entity analytics

The IBM Counter Financial Crimes Management solution delivers a comprehensive array of analytical and investigative capabilities that work together as a single, integrated solution within a common framework and data model.

Identity and relationship disambiguation: To help financial institutions recognize and mitigate the incidence of fraud, deception and collusion, IBM Counter Financial Crimes Management provides identity and relationship disambiguation technology based on context accumulation principles along with complex event processing (see Figure 2).

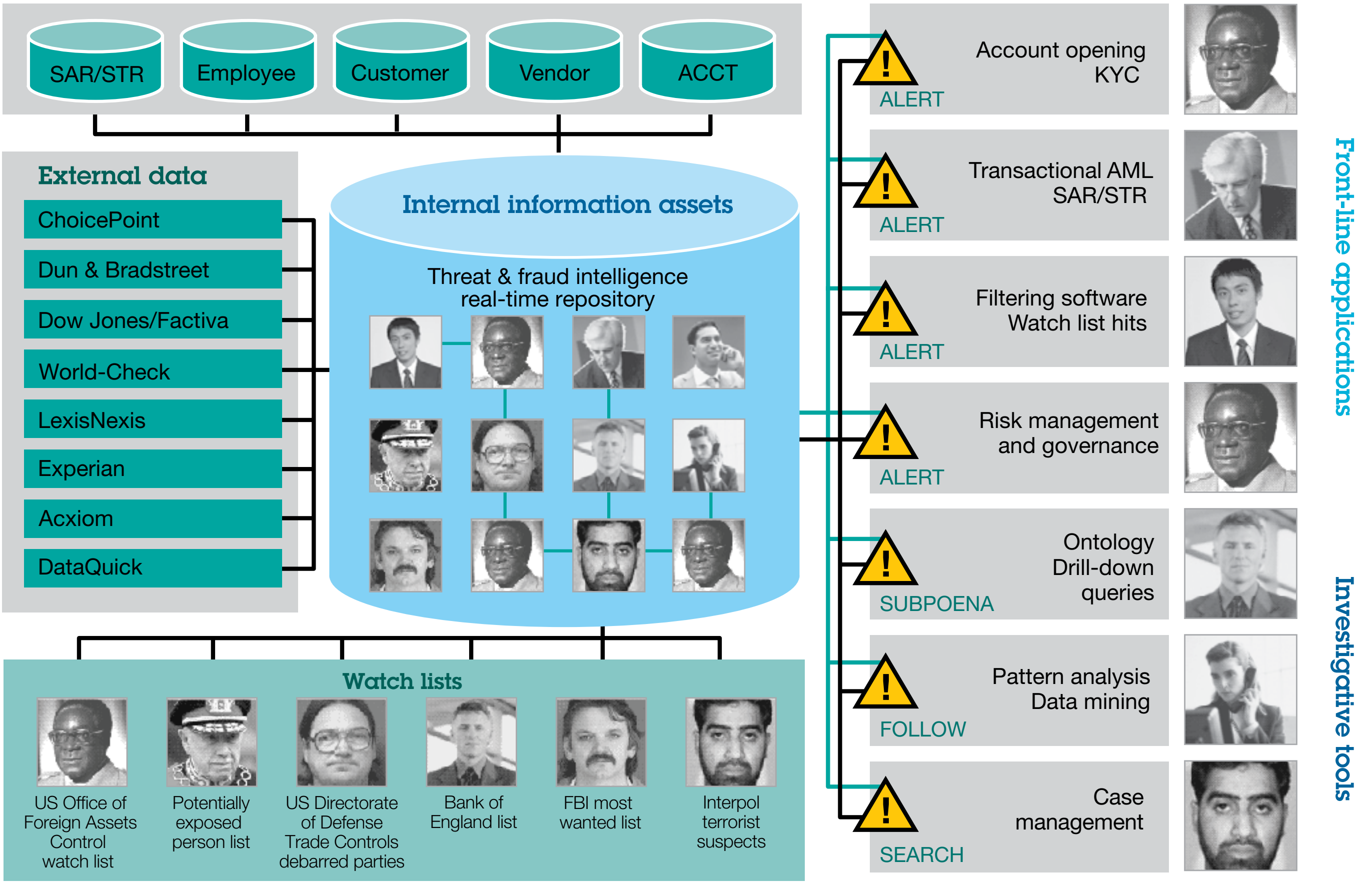
SAR/STR
Employee
Customer
Vendor
ACCT
External data
ChoicePoint
Dun & Bradstreet
Dow Jones/Factiva
World-Check
LexisNexis
Experian
Acxiom
DataQuick
Internal information assets
Threat & fraud intelligence real-time repository
Watch lists
US Office of Foreign Assets Control watch list
Potentially exposed person list
US Directorate of Defense Trade Controls debarred parties
Bank of England list
FBI most wanted list
Interpol terrorist suspects
ALERT
Account opening KYC
ALERT
Transactional AML SAR/STR
ALERT
Filtering software Watch list hits
ALERT
Risk management and governance
SUBPOENA
Ontology Drill-down queries
FOLLOW
Pattern analysis Data mining
SEARCH
Case management
Front-line applications
Investigative tools

Figure 2. As data from multiple sources is pieced together over time, the entity analytics engine within IBM Counter Financial Crimes Management creates rich visualizations to show who is who, who knows whom and who’s doing what.

Context Computing at work: MoneyGram International

By resolving entities and relationships with entity analytics, MoneyGram International managers can better understand who is using the company's services. This knowledge has helped them prevent more than USD37.7 million in fraudulent transactions, reduce customer fraud complaints by 72 percent and quickly address regulatory requirements. Learn more at ibm.com/software/businesscasestudies/us/en/corp?synkey=Y423188O11007S71

The solution uses entity-centric learning when comparing new data records against context. Entities comprise multiple data records, each of which contains its own unique attributes. New records are compared to all of the entity's attributes, even if those attributes were sourced from different records.

Continuous learning: Determining an identity involves making assertions based on context and using those insights for downstream analysis. When new information determines that a previous assertion is no longer valid, IBM Counter Financial Crimes Management will automatically correct the assertion and create an audit trail so overseers can track the changes made to each record.

Rapid risk scoring: IBM Counter Financial Crimes Management incorporates rapid risk scoring capabilities that help financial institutions perform sanctions screening and reduce false positives by identifying legitimate transactions quickly.

Data set mapping: The solution can map internal and external data sets (including unstructured data). These capabilities provide an enhanced understanding of customers and their business relationships while creating a network link graph for further analysis.

Historical recall: Fully attributed historical recall enables banks to get context on the sources of information. Each data record comes from a unique source; the system remembers what the original record looked like and where it came from. This capability helps investigators completely understand the analytics and make the results actionable.

Customers, relationships and context: Critical for crime prevention

With greater insights into customers, relationships and context, financial institutions may gain significant regulatory, operational and technology benefits. More accurate results help reduce regulatory risks. In addition, improvements in the effectiveness and efficiency of anti-fraud and AML initiatives can reduce false positives. Once they achieve clarity into customer behaviors and relationships, financial institutions can leverage predictive analytics technologies to perform more effective risk scoring. Analyzing false positives and negatives enhances predictive analytics and improve risk scoring for future transactions. In this way, IBM Counter Financial Crimes Management with entity analytics enables financial organizations to continually learn and expand their financial crime prevention strategies.

For more information

To learn more about IBM Counter Financial Crimes Management solution with entity analytics, please contact your IBM representative or visit: www.smartercounterfraud.com

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Analytics
Route 100
Somers, NY 10589

Produced in the United States of America
June 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

[1] United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime," February 2013, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[2] United Nations Office on Drugs and Crime, "Money-Laundering and Globalization," www.unodc.org/unodc/en/money-laundering/globalization.html

[3] Global Financial Integrity, "Illicit Financial Flows from the Developing World: 2003-2012," December 2014, www.gfintegrity.org/report/2014-global-report-illicit-financial-flows-from-developing-countries-2003-2012

Please Recycle