WHITE PAPER

Raytheon

Total Exposure:

How Data Clarity® is Proving Critical for Fraud Detection and Prevention.

A combination of uncertainty and fear among private companies and government organizations – in addition to a general lack of awareness – limits big data's potential as a fraud investigation tool. Read the following four, compelling stories and find out how readily available technologies are making it easier to comprehend the meaning of the data, and crack down on crime.

Contents

Organizations Fall Short of Fraud Vigilance Due to Big Data Barriers 4

Case 1: Big data "follows the money," exposing laundering scheme 4

Case 2: Deejays' Duplicitous Border Crossings Foiled by License Plate Searches 5

Case 3: Credit Reporting Grounds "Bust-Out" Plot of Travel Agent 6

Case 4: Foreign Entry Information Tracks Suspicious Trail of Terrorism Suspect 7

Organizations Fall Short of Fraud Vigilance Due to Big Data Barriers

Throughout the world, countless banks, insurers and local/state/federal law enforcement agencies are struggling with big data. There's so much of it, after all. Fear and anxiety steadily build as a series of troubling questions emerge: What data will best support our mission? Where do we find it? How do you distinguish good data from bad? Once we have it, how do we make sense of it all – so we can actually do something with it?

Worse yet, there are an abundance of other organizations which haven't even reached this level of initial paralysis. They lack any awareness of the possibilities of big data. To them, it's an esoteric concept, and they're not convinced of its value. They never get off the ground in seriously evaluating its usage, shrugging their shoulders with comments such as, "We've survived without it … Who really needs this stuff?" They never grasp the range of data out there that could assist them greatly in achieving their strategic goals while working far more efficiently and effectively.

Whether it's fear/uncertainty or awareness issues, the outcomes are the same: Analysts at banks, insurers and related companies are vastly limited in their ability to detect and prevent fraud. Local/state law enforcement, U.S. Department of Justice (DOJ) and Department of Homeland Security (DHS) agencies are similarly confined with respect to the pursuit of investigations. Ultimately, the wealth of data repositories and the volume of the information within overwhelms them – to the point where they simply give up. Or they never get started.

At Raytheon, we've seen first-hand how readily available technology tools can extensively enable these organizations to overcome hurdles of fear, uncertainty and a lack of awareness. Ongoing innovation is liberating users with a profound sense of clarity, and big data no longer intimidates them. In fact, they quickly discover that the data is very easy to navigate and comprehend. Most significantly, they take immediate advantage of it. Then, they explore new ways to expand upon their existing data, to capture more of it, "tame" it and then leverage it. When they do, they encounter the same kinds of "success stories" that we have summarized in this report, to elaborate upon the fraud-related problems which organizations face every day. They illustrate the immense supply of data resources that can directly address pain points, and how the ensuing clarity empowers users to detect and prevent crime and/or swiftly close cases. To learn more, read on:

This amounts to a tremendous undertaking, for certain. To ensure success, the following "key components" as issued by DISA will drive JIE:

Case 1: Big data "follows the money," exposing laundering scheme

SUMMARY

Crooks realize that you don't commit fraud or embezzlement with "one big job." They prefer to stay in the shadows, to conduct a steady series of deceitful claims or transactions for relatively modest sums. Frequently, they succeed because current checks and controls are not configured to recognize the telltale signs or utilize the appropriate datasets. Also, investigators may be wary of employing big data searches due to the staggering amount of information they contain and the perceived difficulty in finding precisely what they need. But when executed properly, a knowledgeable analysis of revealing patterns can serve as a shortcut in confronting criminal behavior.

THE CASE

In San Antonio, Texas, Tom worked as a clerk in a check-cashing office that catered to immigrants who would send funds to their home. On the first of every month, a customer named Carlos came in to transmit a small sum of money to his family in Central America. Over time, a casual friendship developed between Tom and Carlos. However, Carlos lost his job at the local meat-packing plant due to a massive corporate furlough. But he continued to send money abroad regularly, and his transactions even increased to noticeably larger sums. Tom grew suspicious. When he asked about the larger payments, Carlos told him he had won a lot of cash in the lottery. Somewhat skeptical, Tom alerted the company's compliance office, which sought to monitor Carlos' activity. They instructed Tom to document for them totals for Carlos' future transactions, his address, driver's license and Social Security number.

USING BIG DATA: UNCOVERING THE SHADY ACTIVITY OF A "DEAD MAN"

The thought of accessing billions of records from thousands of data bases can create a daunting challenge. But it doesn't have to be an ordeal. Analytics requires creative thinking and the ability to ask the right questions to identify patterns of interest, in this case, for possible laundering. But this allows you to "go where you need to go" as opposed to sorting through endless proverbial haystacks. For example, if one person is linked to two or more addresses, you need to know whether that is an important pattern in the investigation. The subject may have recently moved from one location to another or bought a second home. A check of land sales can validate the behavior. But if the owner routinely makes similar insurance claims on both properties, the claims could indicate fraud.

A review of Department of Motor Vehicles records confirmed an address and valid driving permit for Carlos. Investigators then enlisted a multi-source, big data exploratory and analytics platform to help them unearth information in support of the case. The platform also gave analytics teams direct access to hundreds of data bases.

These data bases included the National Sex Offender Registry; terrorist watch lists including the Office of Foreign Assets Control (OFAC); and arrest reports from counties and municipalities. Analysts drew a link chart, then ran a simultaneous search of multiple data bases to gather additional details. One of the data sources was the Social Security Death Index (SSDI), which updates records of deceased persons. According to the SSDI search, Carlos' Social Security number was registered to a man who died in recent years.

OUTCOME

The SSDI data gave authorities sufficient cause to arrest Carlos. During questioning, he confessed to having been recruited into a laundering ring after he lost his job at the plant. The money he sent abroad came from illicit drug deals and was deposited by a cousin into an off-shore account, and later returned to the U.S. in the form of legitimate investments in American businesses. Although the SSDI contains millions of records, the big data exploratory and analytics platform's selective discovery of non-obvious relationships instantly turned up key information in an easy, user-friendly manner. In one central location, it produced targeted results and visualizations faster and more accurately – with an entirely interactive and all-encompassing approach – than if the authorities tried to access the required data on their own.

"Instead of having to do one, two or 12 queries with a bunch of disparate data sets," said one investigator, "we can query hundreds of sources with one click of the button."

Case 2: Deejays' Duplicitous Border Crossings Foiled by License Plate Searches

SUMMARY

On a typical day last year, U.S. Customs and Border Protection (CBP) agents admitted more than 992,000 people at the nation's nearly 330 land, air and seaports[1], and apprehended or arrested 1,175 people at or between U.S. ports of entry. Located just north of the U.S.-Mexico border, San Ysidro, Calif., serves as the gateway to Tijuana and the Baja Peninsula in Mexico, and remains one of the busiest land crossings in the world. It's also a favorite transit point among drug smugglers. Agents use every means at their disposal – including License Plate Reader (LPR) tracking and ancillary data bases – to thwart such crimes.

THE CASE

Brothers Juan and Ernesto, both native-born Americans, regularly crossed the U.S.-Mexico border at the San Ysidro checkpoint several times a month. This wasn't considered unusual for two men who told authorities they were freelance radio deejays for a small Spanish-language station in Los Angeles, and sought to tape music and interviews of Tijuana bands for air play. CBP agents routinely inspected their audio equipment and never found anything out of the ordinary, only tapes of Latin music and talk. Yet, for two men who were supposed to be on-air personalities (thus, in essence, professional communicators), they failed to make eye contact and were ill at ease during a standard traffic backup. CBP agents needed to know more about the pair and the true purpose of their frequent crossings.

USING BIG DATA: TRAVEL PLANS PERMANENTLY SCUTTLED

License Plate Readers (LPRs) installed at all U.S. crossing points capture the numbers and letters on each vehicle's license plate. They produce by far the largest of big data sets because of the associated high volume, constant changes and real-time assessments of each car. Based on the uniqueness of an LPR-scanned license plate, the information provides law enforcement with transactional events – dates, times and ports of entry – determining the vehicle's crossing pattern. When LPR query findings are cross-referenced with Department of Motor Vehicles records and other resources, the CBP can review the entire history of the car.

In this case, the LPRs verified that the brothers were making regular crossings, as the suspects contended. But they did so at odd intervals, in the early evening on occasions and before dawn on others, and they often crossed at different border ports.

1 Source: http://www.cbp.gov/newsroom/stats/on-a-typical-day-fy2013

However, the brothers averaged less than 24 hours in Mexico before crossing back into the U.S., too brief for them to tape as much music and interviews as they claimed. And while the brothers listed their home and place of work as Los Angeles, their license plate was registered to an address in the Sacramento area, some 520 miles to the north. Such anomalies called for a thorough search of the vehicle.

OUTCOME

There is no one single pattern to confirm suspicious behavior, but rather an alignment of risk factors that are interpreted within the context of the environment. Because the San Ysidro border crossing allows for rapid access in and out of Tijuana, CBP agents maintain a high level of vigilance for drug smuggling into the U.S. and bulk cash smuggling into Mexico, where banking laws are less stringent than U.S. institutions. The lax standards pave the way for the laundering of large sums of cash from drug sales.

Analyzing LPRs in conjunction with other big data sources presents telling patterns and predictive insights. Authorities can call up content from state and local sources (driver information, arrests, IDs, etc.), task forces and operations such as the Transaction Record Analysis Center (TRAC) and federal sources like the Financial Crimes Enforcement Network (FinCEN), where data from Currency Transaction Reports (CTR), Suspicious Activity Reports (SARs) and Money Services Business (MSB) registrations isolates behaviors which may warrant an extensive search of a vehicle.

In investigating Juan and Ernesto, CBP agents concluded that the vehicle represented a high-risk situation because the address on the vehicle registration was greater than 500 miles from the port of entry, and there were routine crossings from multiple ports. Checks of data from TRAC, CTR, SAR and MSB uncovered moderate sums of cash being regularly deposited weekly into a bank in Sacramento located not far from the address on the vehicle's registration. Upon a close examination of the vehicle, officials found a large cash stash in tens and twenties hidden in a false bottom under the trunk. They arrested the brothers, and charged them with money laundering.

Case 3: Credit Reporting Grounds "Bust-Out" Plot of Travel Agent

So-called "bust-out schemes" signify a growing area of financial fraud affecting financial institutions and the public. Despite the best efforts of law enforcers and regulators, monetary losses from such scams continue to increase and those losses are being passed back to consumers in the form of higher fees.

SUMMARY

Bust-outs are difficult to detect. Here's how they work: The perpetrators first build up a track record of good credit/payment histories for an account. Then, they "bust out" by initiating chargebacks and stopping payments, and abandon the account. By shutting down and fleeing the jurisdiction, they leave their creditors with substantial debt.

THE CASE

Kim operated a small travel agency that catered to the local immigrant community, mostly selling airline tickets to clients looking to visit their home country. Initially, the agency did well, but it suffered during the recent recession. So she turned to her credit-industry savvy part-time assistant to break out of her predicament. Together, they began to sell airline tickets at greatly reduced rates to the community and even to other agencies in their area.

A credit organization acting as an industry clearinghouse requires its travel agency members to remit payment for tickets sold weekly. For about one year, Kim's agency made steady payments. During this same period, she gradually increased her ticket sales figures. When the agency reached weekly sales of at least $100,000, Kim paid with a check drawn on a banking account with insufficient funds. That deliberate tactic extended the time Kim had to pay and also gave her another four to six weeks to collect more funding from ticket sales. When the clearinghouse finally closed her agency's account, the bust-out was complete and Kim and her assistant prepared to leave the country.

USING BIG DATA: DUE DILLIGENCE THROUGH CREDIT REPORTING

The indicators for bust-outs are typically problematic to detect because the timing of the fraudulent act is uncertain and abrupt. In addition, the target of the scheme is often a large financial institution with hundreds of clients and many millions of dollars in daily transactions. Perpetrators can further cloud their intentions by distributing operations throughout multiple organizations. In 2013, Kim's clearinghouse processed $86 billion worth of tickets for 190 carriers and some 9,400 travel agencies with 15,000 points of sale.

Recent advancements in analytics are giving credit providers the ability to instantly check the transaction/payment history of prospective merchants, because all fraud data is secured in a global and neutral data base. This permits participants to post and access the latest information, and to conduct due diligence prior to accepting prospective merchants. Reporting can capture behaviors such as suspicious credit line/balance increases and unusual purchases. By generating the wider perspective that analytics can bring, bust-out predictors are identified before the crime is accomplished and protect financial institutions from substantial losses.

OUTCOME

Using analytics and a bust-out scoring algorithm created by a credit reporting agency, Kim's plot was revealed just days before she and her assistant were scheduled to fly out of the country. Both were taken into custody.

Case 4: Foreign Entry Information Tracks Suspicious Trail of Terrorism Suspect

SUMMARY

Basic information on all foreign visitors arriving in the U.S. by air or sea was once was reported by the traveler on a paper form. CBP now gathers this from electronic passenger manifests transmitted by the carrier, a process that facilitates security and reduces costs.

The data includes names, addresses, birth dates, countries of citizenship, passport numbers, flight numbers or shipping line names and ports of embarkation, and addresses while in country. For most travelers, the required information is innocuous and routine. But when coalesced with other data – such as hotel stays, car rentals and financial transactions – the results can reveal a number of patterns to spot illegal entrants and dubious behaviors, such as the use of multiple passports by a single individual.

THE CASE

Mohammad, who listed his occupation as a courier from a south Asian nation, made numerous trips to New York City, transiting through a Middle East emirate, where he would spend a week or so before flying to the U.S. On each visit, his data was recorded. Because he came from a high-risk area, Mohammad's information was processed through the Treasury Enforcement Communications System (TECS), a DHS mainframe computer data base. Findings showed that Mohammad's airline, flight number and U.S. arrival port were always the same. But he never stayed at any New York hotel twice and often there were days which were unaccountable.

USING BIG DATA: "GARBAGE" DATA RED FLAGS THREATENING INTENTIONS

In scrutinizing the collected information, analysts routinely aggregate query findings and discard what they consider to be "garbage data." In this investigation, there were a number of minor inconsistencies in the spelling of "Mohammad," which could be attributed to the applicant's poor knowledge of English or to the carrier's error. Although results showed that Mohammad's place and date of birth were consistent throughout, he listed a dozen different passport numbers on his more than 60 entries during the previous five years. On one recent trip, for example, he listed multiple passport numbers on his arrival and departure forms. Were they stolen or counterfeit, or the product of lax passport application processing by a developing nation with weak controls and inadequate computerized data collection? When checked against Mohammad's visa applications, the inconsistencies – and the possibility of potential terrorism – could not be overlooked.

OUTCOME

Collating the data from DHS and other international law enforcement and intelligence organizations, a national anti-terrorism team learned that the address of Mohammad's courier business was that of a vacant warehouse in a rural village far from his homeland's capital. Before he could leave the country again, Mohammad was taken in for questioning. When confronted with the evidence and additional inconsistencies in his data, he confessed to joining an international anti-American group and, while in the U.S., updated like-minded individuals with news and instructions from the faction. His visa was revoked, his name was placed on a no-fly watch list and he was debarred from entering the country.

Conclusion

Complete Clarity establishes big data vision. Before the Digital Age, it was much easier for fraudsters to "hide in plain sight," covering their tracks while stealing other people's money, and appearing to live the lives of honest citizens. Today, analytics converts seemingly intangible electronic data into a remarkably lucrative asset, one that pays for itself – and far beyond – as it takes voluminous information from varied sources and promptly identifies the factual threads which call out criminal intent.

Raytheon is leading the path to total visibility into illegal activity to support analysts and investigators at banks, insurers, law enforcement/DOJ agencies and the DHS. The Data Clarity Platform is a potent, multi-source, big data exploratory and analytics tool that enables our customers to unearth evidence which secures criminal convictions. It also delivers a direct connection to the Raytheon Data Clarity Data Center, which allows teams access to hundreds of immediately actionable, impactful data bases.

As a result, uncertainty about data among our customers gives way to absolute confidence. It transforms anxiety and fear of once-unmanageable information into an assured state of command over it. It sheds any inhibitive lack of awareness within the enterprise, and replaces it with limitless knowledge.
And the transition to this state is simpler than you'd think. To request a Data Clarity demonstration and to learn how your organization can benefit from Raytheon's data discovery and investigative analytical capabilities, call 1-866-230-1307.

About Raytheon Cyber Products

Raytheon Cyber Products, a leading provider of Commercial-Off-The-Shelf (COTS) cyber security solutions for government and industry, is a wholly owned subsidiary of Raytheon Company. Founded on deep knowledge of cyber security stemming from the U.S. Department of Defense and the Intelligence Community, Raytheon Cyber Products has evolved into a company that both commercial and government enterprises rely on to ensure the security of their most critical cyber assets. The company's broad portfolio of products addresses a variety of cyber challenges that organizations face today including insider threat, secure information sharing, data loss prevention, and data analysis. With over 20 years of collective experience in delivering the highest caliber security solutions, customers trust Raytheon Cyber Products to deliver solutions that are innovative, flexible, and scalable, meeting their security needs today and in the future. The company has over 300 employees with headquarters in Herndon, Virginia.

For further information contact:

Intelligence, Information and Services
Cyber Products
12950 Worldgate Drive, Suite 600
Herndon, Virginia
20170 USA
866.230.1307

www.raytheon.com/cyberproducts

Raytheon

Customer Success Is Our Mission