Volume 1, Issue 2
May 2009

The Idola Report

Information to Vision

Excellence, reliability, and value are core principles followed by Idola while working with its clients and partners. This newsletter will provide current information to help financial institutions meet their risk and compliance mandates. It is with current, meaningful information that appropriate vision is developed to meet today's challenges.

To subscribe, add a colleague, or to opt out of the Idola Report, simply send an email request to: newsletter@idolainfotech.com.

Insurance Industry – Suspicious Activity Reporting

The overall volume of Suspicious Activity Reports from the insurance industry continues to increase since the mandated suspicious activity reporting rule became effective on May 2, 2006. FinCEN released an assessment of the SARs filed by the Insurance Industry over their first year from the date of mandated suspicious activity reporting.

For the complete assessment, click on:
http://www.fincen.gov/news_room/rp/reports/pdf/Insurance_Industry_SAR.pdf

Anti-Money Laundering Program for Hedge Funds

On January 20, 2009, Senators Charles Grassley (R-IA) and Carl Levin (D-MI) introduced the Hedge Fund Transparency Act, which, if enacted, will close previous loopholes allowing hedge funds to avoid Securities and Exchange Commission (SEC) supervision and will mandate establishing and implementing an anti-money laundering (AML) program and reporting suspicious transactions.

Please refer to the below, (Section 4 for AML related content) of the bill:
http://levin.senate.gov/newsroom/supporting/2009/hedgefundsbill.012909.pdf

Copyright 2009, Idola Infotech, LLC

IDOLA
INFOTECH

Volume 1, Issue 2
May 2009

The Idola Report

Connections of Mortgage Fraud with other Financial Crimes

As we mentioned in the last issue, though organizations of many financial institutions have separated the functional management of risk, compliance, and fraud in many respects these functions are complimentary and only with their common oversight will the risk be appropriately mitigated. Consequently, software solutions have developed along the same dividing lines resulting in sub optimal support for these essential activities.

FinCEN, recently released a report on the connection between Mortgage Fraud and other financial crimes, like check fraud, structuring to avoid currency transaction reporting, money laundering and others.

Please click on the following for the complete report:
http://www.fincen.gov/news_room/rp/files/mortgage_fraud.pdf

Remote Data Capture Risk Management

FDIC released a letter to financial institutions providing guidance that a financial institution offering remote data capture (RDC) should have sound risk management and mitigation systems in place and should require adequate risk management at customer locations. Prior to implementing RDC, and periodically thereafter, management should conduct a risk assessment to identify the related types and levels of risk exposure.

For complete details, click on:
http://www.fdic.gov/news/news/financial/2009/fil09004a.pdf

Vulnerabilities of Casinos and Gambling Sector

Financial Action Task Force (FATF) has recently released a report on the gaps in awareness of Money Laundering typologies in the cash intensive, competitive in growth and vulnerable to criminal exploitation sector of Gambling and legal casinos .

For complete details, click on:
http://www.fatf-gafi.org/dataoecd/47/49/42458373.pdf

Copyright 2009, Idola Infotech, LLC

IDOLA INFOTECH

Volume 1, Issue 2
May 2009

The Idola Report

International ACH Transactions (IAT) Implications

International ACH Transactions (IAT) requirements, whose primary purpose is to align NACHA rules with OFAC compliance requirements, are going to be available from September 2009. All U.S. financial institutions are affected by the new NACHA rule requirements for IAT, even those that do not currently send or receive international ACH transactions as any financial institution may potentially receive an IAT entry.

For further information, click on:
http://www.frbservices.org/eventseducation/education/iat_originating_institution.html

Red Flags

If you are a creditor or financial institution with covered accounts, your deadline of May 2009 for developing and implementing a written Identity Theft Prevention Program is fast approaching. This program must be designed to prevent, detect and mitigate identity theft in connection with the opening of new account and operation of existing ones..

For details, click on:
http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf

Quantifying False Positives

By Sunil Choudhary, CAMS, CISA, CISSP, a principal of enCautus, a risk and compliance consultancy, sunilc@encautus.net

False positives are an unavoidable problem in transaction monitoring. Research and analysis into the causes of excessive false positives can yield significant savings of effort and costs. However, in order to be able to control the occurrences of false positives, it is imperative to be able to measure and quantify them. In this article, I present a way to quantify false positives using a technique called Bayesian Inference.

Bayesian Inference

The Bayes theorem has become well known in recent times because it is used extensively in e-mail spam control tools.

Thomas Bayes was a British mathematician and Presbyterian minister in the early 18th century. His theorem states:

Copyright 2009, Idola Infotech, LLC

The probability of any event is the ratio between the value at which an expectation depending on the happening of the event ought to be computed, and the chance of the thing expected upon its happening.

Obtuse as most mathematical theorems are, this one can be applied to a variety of natural occurrences. We will use this Bayesian inference technique to quantify false positives.

(I must credit Eliezer Yudkowsky for his seminal articles on this topic and encourage readers to acquaint themselves with his work).

Riddle

In a bank 1% of transactions are suspicious, and just 80% of the suspicious transactions will be flagged as such by their Transaction Monitoring System (TMS). However 10% of transactions that are not suspicious will also be flagged as suspicious by the TMS. A transaction at this bank is flagged as suspicious. What is the probability that the transaction is actually suspicious?

Please spend a couple of minutes in figuring it out.

Analysis

Before the TMS screening, let us say the bank had 100,000 transactions in a given month. We will divide the transactions into two groups:

Group 1: 1,000 transactions that are suspicious.
Group 2: 99,000 transactions that are not suspicious.

After the TMS examines the transactions we get four sets of results:

Set A: 800 transactions which are *suspicious* and are *flagged.*
Set B: 200 transactions which are *suspicious* but are *not flagged.*
Set C: 9,900 transactions which are *not suspicious* but are *flagged.*
Set D: 89,100 transactions which are *not suspicious* and are *not flagged.*

The total number of transactions is 100,000. The sum of Set A and Set B, the sets with *suspicious* activities belong to Group 1; and the sum of sets C and D, the groups without suspicious activity, belongs to Group 2.

The proportion of the suspicious activity (Set A + Set B) within the complete set of transactions Sets (A + B + C + D) is the same as the 1% probability that an

Copyright 2009, Idola Infotech, LLC

activity is suspicious: (800 + 200) / (800 + 200+ 99,000 + 89,100) = 1,000 / 100,000 = 1%.

The proportion of suspicious activity which is flagged by TMS, within the group of *all* flagged activity, is the proportion of A within (A + C): 800 / (800 + 9,900) = 800 / 10,700 = 7.5%.

Therefore, the percentage of false positives in this example is **92.5%** (results have been rounded up). This is an extreme example. If 1% of all activities in a bank are suspicious, it is in real trouble. However, in a few locations where we ran an analysis using realistic numbers, false positive proportions were much higher.

Results
Three key numbers are used in the above inference:
P(x): percentage of transactions which are *suspicious* and *flagged* as suspicious
P(y): percentage of transactions which are *not suspicious* but are *flagged* as suspicious
P(z): percentage of transactions which are *suspicious* but *not flagged* as such.

The P(y) is easy to obtain, but P(x) and P(z) are more difficult. There is a lot of statistics available on the Internet (one data-rich site is http://www.fincen.gov/sars/sar_by_numb_11.pdf), but it is hard to find a number that is right for your institution because of the large number of variables. For example, in year 2007 depository institutions filed 649,176 suspicious activity report (SARS), but it will be hard to say that all suspicious activities were reported or that all the SARS filed were truly suspicious. A realistic process to use is to analyze the past results of your TMS and arrive at a reasonable estimate.

Next step
There is a correlation between P(x) and P(y). If you want to increase P(x) -- catch as many suspicious transactions you can -- it will inevitably increase P(y), the number of transactions that are not suspicious but are flagged as such. But as an exercise, measure the impact of reducing P(y) by 10% while keeping the P(x) at its original number. Redo the calculation. The reduction in the number of false positives is significant.

Copyright 2009, Idola Infotech, LLC

IDOLA INFOTECH

Volume 1, Issue 2
May 2009

The Idola Report

Share Your Knowledge

Knowledge sharing among peers is an essential service that helps us all navigate through our responsibilities in our risk and compliance professions. The Idola Report is dedicated to facilitating this valuable service. If you have information that you believe should be shared with other subscribers of the Idola Report or would like to submit an article for publication, please contact Sal Cangialosi at the address below.

About Idola

Idola Infotech was founded in 2002 by a team that specialized in software product development and the deployment of complex technology projects. Its management team consists of banking experts, leaders of the regulatory compliance market, and senior technology specialists. They have developed commercial products for one of the largest vendors of financial services software. Project management experience has been earned across a wide range of financial institutions from some of the largest in the world to small community banks. Idola has implemented and deployed software solutions domestically and internationally earning its reputation for ***excellence, reliability, and value.***

Products and Services

Technology Services for Financial Institutions
Regulatory Compliance Consulting
Compliance Process Outsourcing
Independent Review of AML Compliance
Financial Services Vendor Support
Data Research and Aggregation
SWIFT Support Services and SWIFT Message Director

Contact

For further information contact:
Salvatore Cangialosi
Idola Infotech, LLC
120 Wood Avenue South, Suite 407
Iselin, NJ 08830
Tel: 732-470-4047
Email: scangialosi@idolainfotech.com
Web: www.idolainfotech.com

Copyright 2009, Idola Infotech, LLC