Reducing "False Positive" Determinations in Fraud Detection

INTRODUCTION

Over the past decade, fraud and identity theft have increasingly plagued consumers, businesses, and financial institutions.[1] The IRS has also been impacted. A 2015 Treasury Inspector General for Tax Administration (TIGTA) report found that approximately 1.5 million returns for tax year (TY) 2010 with characteristics of identity theft were processed undetected, with potentially fraudulent refunds totaling $5.2 billion issued.[2] In order to detect and prevent identity theft and potentially false wages and withholdings, the IRS established a complicated screening process.[3] When a return is flagged by one of the multiple systems that scrutinize returns for characteristics of refund fraud or identity theft,[4] the refund is stopped from being issued until the taxpayer can authenticate his or her identity or until the information on the return can be verified. Some returns flagged by these systems turn out to be false positives.[5]

The National Taxpayer Advocate has consistently advocated for taxpayers whose legitimate refunds have been wrongly selected and unreasonably delayed with IRS Refund Fraud and Identity Theft Programs.[6] This literature review explores the acceptable false positive rates in the public and private sectors and steps that can be taken to reduce false positive rates.

DISCUSSION

A survey of literature shows that the issue of false positives is common in both private and public sectors which use technology to gather and analyze information to detect and address potential problems. For instance, modern medical technology allows conducting biopsies and other procedures to detect potential health issues, and then uses that information to determine potential treatment options.[7] Another example includes the United States Department of Defense gathering intelligence information to identify high

1 American Bankers Association (ABA), *Banks Stop $11 Billion in Fraud Attempts in 2014* (Jan. 27, 2016), http://www.aba.com/press/pages/012716depositsurvey.aspx (While attempted fraud against bank deposit accounts reached $13 billion, banks' prevention measures stopped $11 billion in fraudulent transactions). An estimated 17.6 million persons, or about seven percent of U.S. residents age 16 or older, were victims of at least one incident of identity theft in 2014. *See* Erika Harrell, *Victims of Identity Theft*, 2014, Bureau of Justice Statistics (Sept. 2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf.

2 Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 24, 2015).

3 The IRS Return Integrity & Compliance Services (RICS) uses three independent systems to identify returns when it suspects identity theft has occurred or that the return is fraudulent. These systems are the Dependent Database (DDb), the Return Review Program (RRP), and the Electronic Fraud Detection System (EFDS).

4 The IRS has distinct screening processes for identity theft and refund fraud. For purposes of this report, we will refer to refund fraud in its broadest sense, to include identity theft as a subset of refund fraud. *See also* National Taxpayer Advocate 2015 Annual Report to Congress 45-55 (Most Serious Problem: *Revenue Protection: Hundreds of Thousands of Taxpayers File Legitimate Tax Returns That Are Incorrectly Flagged and Experience Substantial Delays in Receiving Their Refunds Because of an Increasing Rate of "False Positives" Within the IRS's Pre-Refund Wage Verification Program*).

5 A false positive occurs when a system selects a legitimate return and delays the refund past the prescribed review period. IRS, *IRS Return Integrity & Compliance Services (RICS): Update of the Taxpayer Protection Program (TPP)*, 4 (Aug. 17, 2016).

6 *See, e.g.*, National Taxpayer Advocate 2015 Annual Report to Congress, 45-55, 180-87; National Taxpayer Advocate 2014 Annual Report to Congress vol. 2, 44-90; National Taxpayer Advocate 2013 Annual Report to Congress 75-83; National Taxpayer Advocate 2012 Annual Report to Congress 42-67, 95-110; National Taxpayer Advocate 2011 Annual Report to Congress 48-73; National Taxpayer Advocate 2009 Annual Report to Congress 307-17; National Taxpayer Advocate 2008 Annual Report to Congress 79-94; National Taxpayer Advocate 2007 Annual Report to Congress 96-115; National Taxpayer Advocate 2005 Annual Report to Congress 25-54, 180-91; National Taxpayer Advocate 2004 Annual Report to Congress 133-36; National Taxpayer Advocate 2003 Annual Report to Congress 175-81.

7 *False-positive Results Are Common with Cancer Screening*, CancerConnect.com, http://news.cancerconnect.com/false-positive-results-are-common-with-cancer-screening/ (last visited Dec. 5, 2016).

value military targets.[8] Inevitably, there are instances in which certain presumably true information turns out to be false (*e.g.*, a biopsy that is positive turns out to be false, or a location that is identified as a military installation turns out to be a civilian location).[9] These instances are commonly referred to as a "false positives."[10] Conversely, there are situations where something is identified as not possessing the selected characteristics, but the determination is false (*e.g.*, a biopsy that is actually positive is deemed negative). This is commonly referred to as a "false negative."[11] The two examples above illustrate how acting on a false positive or not acting on a false negative comes with a very high cost of losing life, causing injury, or destroying property.

Of course, acting or not acting on false information may not always come at such a high cost, but nonetheless, the consequences can be significant. Some more comparable examples to tax administration, such as the financial sector, track their false positive rates to determine how effective their systems are in accurately identifying fraud or identity theft. In the context of commerce and the financial industry, not detecting fraudulent purchases or transactions may result in the loss of hundreds of thousands of dollars, not to mention customer loyalty. However, an overly inclusive fraud detection system that results in a high number of legitimate transactions being declined also can come at a high financial cost.

For example, sales that were blocked by the credit card companies' fraud detection systems amounted to $118 billion in 2014, while the cost of real card fraud only amounted to $9 billion for the same year.[12] Further, the percentage of consumers affected by false-positive declines is three times greater than the percentage affected by card fraud. Fifteen percent of all cardholders have had at least one transaction declined because of suspected fraud in the past year, compared to just four percent of defrauded consumers.[13] Two-thirds of cardholders who were declined during an e-commerce (electronic) transaction or m-commerce (mobile) transaction reduced or stopped their patronage of the merchant following a false-positive decline (versus 54 percent for all declined cardholders).[14]

Downstream Costs of Fraud

In regard to losses due to identity theft or fraud, the monetary cost can go far beyond the actual amount stolen. In fact, one source stated that losses caused by internal or external fraud costs five times the original amount lost:

- One dollar in actual cash or property value is lost;
- A second dollar is spent identifying how the crime was committed;

8 Neta C. Crawford, *Targeting Civilians and U.S. Strategic Bombing Norms: Plus ça Change Plus C'est la Même Chose*, *in* The American Way of Bombing: Changing Ethical and Legal Norms, from Flying Fortresses to Drones 64, 81 (Matthew Evangelista & Henry Shue, eds., 2014) ("First, algorithms that estimate noncombatant killing for preplanned strikes were employed much more widely than in previous conflicts. These algorithms are a set of decision rules, formulas, and inputs used to calculate risk and likely harm to noncombatants. And second, there was a threshold of risk to noncombatants that was considered acceptable given the understanding of military necessity and the estimated risk to U.S. forces.").

9 Matthieu Aikins, *Doctors With Enemies: Did Afghan Forces Target the M.S.F. Hospital?*, The N.Y. Times, May 17, 2016, http://www.nytimes.com/2016/05/22/magazine/doctors-with-enemies-did-afghan-forces-target-the-msf-hospital.html?_r=0.

10 Generally speaking, a false positive is a test result which incorrectly indicates that a particular condition or attribute is present.

11 "With simple matching approaches, there is a direct relationship between the number of false positives and the number of false negatives: decreasing one generally leads to an increase in the other. Fortunately, there are ways of decreasing the number of false positives without increasing the risk of false negatives. The burden of false positives can be further alleviated by adopting an approach and process that focuses effort on the highest areas of risk and removes wasted effort." Oracle, *Reducing False Positives Without Increasing Regulatory Risk*, 2 (Sept. 2011).

12 *Fraud Losses and False Positives: The Numbers*, SecuredTouch (Dec. 2015).

13 Al Pascual *et al.*, Javelin, *Overcoming False Positives: Saving the Sale and the Customer Relationship*, 4 (2015).

14 *Id.*

- A third dollar is spent in identifying who committed the crime;
- A fourth dollar is spent prosecuting the person who committed the crime; and
- A fifth dollar is spent in suing the person who committed the crime for the recovery of the money taken.[15]

Both the Financial and Commercial Sectors Have Developed Technology to Better Detect Potential Fraud or Identity Theft in an Effort to Protect Customers and Reduce Direct and Indirect Costs

In commerce, the best practice for merchants is adopting a holistic approach to validation and authorization instead of declining a transaction based on a single suspicious data point.[16] This approach entails analyzing multiple characteristics of a shopper to determine if all the available data indicate the purchase is legitimate. In essence, this approach calls for a customized understanding of each and every transaction.[17] Occasionally, transactions are declined because there is insufficient information to validate the legitimacy rather than actual fraud. Accurately tagging each transaction can help shape future authorization rules and may help decrease the rate of false-positive declines.[18]

In the financial sector, a system developed to detect fraud normally contains the following four elements:

- Detect: predict fraud before it happens;
- Respond: apply new fraud insights;
- Investigate: turn fraud intelligence into action; and
- Discover: leverage existing historical data.[19]

Most importantly, a system should be flexible, adaptable, and continuously changing to meet the various changes in risk.[20] The heart of an efficient fraud prevention solution is a strong analytics engine, which can use the available data intelligently, recognize and identify patterns, provide real time visibility into threats, and signal discrepancies.[21] It should enable the solution to detect and respond swiftly to suspicious or fraudulent transactions.[22]

An efficient fraud detection system includes a combination of these elements:

- *Advanced Analytics:* Critical data drawn from across the enterprise might be centralized in a flexible framework environment that, unlike more limiting relational databases, can accommodate and homogenize multiple data formats. This central "data mart" would also feature multiple analytical capabilities and a variety of tools that make it possible for users to work with analyzed data in a

15 Asad Ali Shah, Deloitte Pakistan, *Good Corporate Governance: Essential to Prevent Conflicts of Interest and Fraud - Pakistan's Experience*, 13, https://www.oecd.org/site/adboecdanti-corruptioninitiative/39367990.pdf.

16 Al Pascual *et al.*, Javelin, *Overcoming False Positives: Saving the Sale and the Customer Relationship*, 6 (2015).

17 *Id.* at 16, 17 (2015).

18 *Id.* at 17 (2015).

19 IBM Software, *Fighting Fraud in Banking with Big Data and Analytics*, 4 (Oct. 2014).

20 Inst. Internal Auditors, *et al.*, *Managing the Business Risk of Fraud: A Practical Guide* (June 2008), http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf.

21 Vasudevan Easwaran, WIPRO, *The Combination to a Safe Future for Banking: Using Technology in The Banking Industry to Prevent Fraud*, 4 (2015).

22 *Id.*

production environment.[23] This type of analytic modeling can help to determine when fraud is identified, and whether this type of fraud is the work of an individual or a criminal organization.[24]

- *Behavioral Analytics:* Each individual customer has his or her own unique banking behavior, consisting of a detailed, multi-faceted combination of timing, sequence, devices, locations, channels, and the financial and non-financial activities performed via those channels.[25] Behavioral analytics solutions are designed to understand the normal behavior of each individual account holder, calculate the risk of each new activity and then choose intervention methods commensurate with the risk.[26]
- *Transaction Analytics:* This technique allows financial institutions to analyze their customers' detailed transaction data over time to gain an understanding of customers' purchasing patterns and behaviors.[27]
- *Anomaly Analytics:* This analytical technique is focused on detecting inconsistencies with previously demonstrated "normal" patterns of behavior. The power of anomaly detection lies in the fact that it doesn't matter how the account is compromised - whether it's a Trojan or other malware, stolen credentials, or social engineering through customer service - the suspicious behavior relative to established norms is what provides a clue or signals that something is amiss. This component is based on a layered security strategy, as called for by the Federal Financial Institutions Examination Council (FFIEC). When (not if, but when) a person attempting to commit fraud gets past one layer (*e.g.*, device password, ID, tokens, out of wallet challenge questions, out of band authentication, or positive pay verification), another confronts him, adding to the effectiveness of the entire security strategy.[28]

Literature shows that using a mix of these fraud detection mechanisms results in a reduction of false positives because if more than one detection method flags the user who is attempting fraud, this is more credible than if only one detection method identifies attempted fraud.[29] This approach is being used in the credit card industry.

Additionally, several sources discuss the importance of communication in an organization regarding what trends are taking place in attempted fraud and identity theft. Designing an organizational structure that allows sharing of information in real time allows all necessary stakeholders to evaluate and adjust an organization's fraud detection systems and filters based on this information. In fact, for this "data mart" strategy to be effective, the organization's IT directors have to accept that some traditional IT implementation and support processes are simply too slow to react to actions of fraud groups.[30] However, having a large number of stakeholders involved in the decision-making process runs a "risk of

23 Deloitte, *The Latest Tools, Tactics for Battling Bank Fraud*, Wall St. J.: CIO J. (May 1, 2014), http://deloitte.wsj.com/cio/2014/05/01/the-latest-tools-tactics-for-battling-bank-fraud/.

24 Robert Griffin, *Combating Payments Fraud in a Big Data World*, BAI Banking Strategies (Mar. 19, 2014), https://www.bai.org/banking-strategies/article-detail/combating-payments-fraud-in-a-big-data-world.

25 Craig Priess, *Behavioral Analytics for Detecting Fraud*, BAI Banking Strategies (Mar. 18, 2015), https://www.bai.org/banking-strategies/article-detail/behavioral-analytics-for-detecting-fraud.

26 *Id*.

27 Dean Nolan, *Combating Fraud with Transaction Analytics* (Apr. 2, 2014), https://www.bai.org/banking-strategies/article-detail/combating-fraud-with-transaction-analytics.

28 Guardian Analytics, *Best Practices for Detecting Banking Fraud*, 2 (2013), http://www.cbai.com/news/Best_Practices_for_Detecting_Fraud_white_paper.pdf.

29 *Fraud Losses and False Positives: The Numbers*, SecuredTouch (Dec. 2015).

30 Deloitte, *The Latest Tools and Tactics for Battling Bank Fraud*, Wall St. J.: CIO J. (May 1, 2014), http://deloitte.wsj.com/cio/2014/05/01/the-latest-tools-tactics-for-battling-bank-fraud/.

over-governance resulting in duplication, inefficiencies, and uncertainty relating to ownership of [fraud detection] issues needing resolution."[31]

How the Australian Taxation Office is Addressing Identity Theft and Fraud

In the tax administration context, the IRS may collaborate with and learn from experiences and mistakes of the Australian Taxation Office (ATO). The ATO has implemented a number of controls and systems to detect potential refund fraud, including analytical models that use behavioral and statistical algorithms to analyze information on income tax returns, business activity statements and other tax forms.[32] However, an Inspector General review of the ATO's integrity refund program found that it was difficult for the risk-based criteria in its system to reflect recent fraudulent activity in real time.[33] This literature review may be helpful for the IRS to identify necessary elements of a robust fraud detection system and learn from private sector and other tax administration's experiences to establish aspirational goals and benchmarks for its fraud detection programs.

LITERATURE REVIEW

1. **ACI Payment Sys.**, ACI Worldwide, *An Industry Guide: Stopping Card Fraud in its Tracks*, 5 (2010), https://www.aciworldwide.com/-/media/files/collateral/aci_stopping-card-fraud-guide_tl_us_1010_4414.pdf.

   "As the number of bank cards and the number of payments made with these cards increase, so too have associated fraud levels including identity theft on cards, stealing of cards in transit/mail, physical theft, counterfeit and skimming. As such, card fraud has become a significant problem for the global retail banking sector. Debit and credit card fraud alone is estimated by Visa and MasterCard to exceed $10 billion worldwide in 2009 and financial institutions are facing an ongoing battle to beat those attempting to commit fraud while protecting their customers."

2. **ACL Servs.**, *Fraud Detection Using Data Analytics in the Banking Industry*, 5 (2014), https://www.acl.com/pdfs/DP_Fraud_detection_BANKING.pdf.

   "A fraud detection and prevention program should include a range of approaches — from point-in-time to recurring and, ultimately, continually for those areas where the risk of fraud warrants. Based on key risk indicators, point-in-time (or ad hoc) testing will help identify transactions to be investigated. If that testing reveals indicators of fraud, recurring testing or continuous analysis should be considered."

31 Inspector-Gen. of Taxation, Austl. Gov't., *Review into the Australian Taxation Office's Compliance Approach to Individual Taxpayers - Income Tax Refund Integrity Program*, 13 (Sept. 2013), http://igt.gov.au/files/2014/11/income-tax-refund-integrity-program.pdf.

32 *Refund Fraud*, Austl. Tax'n Off., https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Refund-fraud/ (last modified Aug. 3, 2015).

33 Inspector-Gen. of Taxation, Austl. Gov't., *Review into the Australian Taxation Office's Compliance Approach to Individual Taxpayers - Income Tax Refund Integrity Program* 10 (Sept. 2013), http://igt.gov.au/files/2014/11/income-tax-refund-integrity-program.pdf.

3. **Akindele R.I.**, *Fraud as a Negative Catalyst in the Nigerian Banking Industry*, 2 J. Emerging Trends in Econ. & Mgmt. Sci. 357, 357 (2011), http://jetems.scholarlinkresearch.com/articles/Fraud%20as%20a%20Negative%20Catalyst%20in%20the%20Nigerian%20Banking%20Industry.pdf.

   "Fraud in the Nigerian Banking Industry before the recent merger and acquisition and recapitalisation efforts was at alarming rate. It has caused many banks to collapse, and many investors and depositors funds were trapped in. In fact it has prevented many banks from achieving their goals and many businesses went into liquidation. Honestly speaking it has become a cankerworm that has eating deep into the vibric [*sic*] of the financial sector of the Nigerian economy. That calls for the need for this study and the purpose of this study therefore is to identify the causes of fraud, measure its impact and identify means of controlling. The study is a survey research and questionnaire was used for the collection of primary data while libraries, journals, write-ups, seminar papers and books by popular authors were used for secondary data. The findings show that lack of adequate training, communication gap, and poor leadership skills were the greatest causes of fraud in Nigerian banking industry. It was concluded that adequate internal control system should be put in place and that workers satisfaction and comfort should be taken care of."

4. **Al Pascual *et al.***, Javelin, *Overcoming False Positives: Saving the Sale and the Customer Relationship*, 3 (2015).

   "Merchants face a serious challenge in today's marketplace as they try to balance the need for strong antifraud measures with consumers' desire for fast, easy, and digital purchases. Quite often, security measures incorrectly flag legitimate transactions, which potentially alienate customers and result in reduced revenue for merchants. One in six (15%) of all legitimate cardholders experienced at least one decline because of suspected fraud in the past year, resulting in a total of $118 billion declined. Unfortunately for merchants, 26% of declined cardholders reduced their patronage of a merchant following a decline and 32% stopped shopping with the merchant entirely."

5. **American Bankers Association (ABA)**, *Banks Stop $11 Billion in Fraud Attempts in 2014* (Jan. 27, 2016), http://www.aba.com/press/pages/012716depositsurvey.aspx.

   "The nation's banks stopped more than $8 out of every $10 of attempted deposit account fraud in 2014, according to the 2015 American Bankers Association Deposit Account Fraud Survey Report. While attempted fraud against bank deposit accounts reached $13 billion, banks' prevention measures stopped $11 billion in fraudulent transactions. Fraud against bank deposit accounts cost the industry $1.9 billion in losses — an increase from $1.7 billion in 2012."

6. **Asad Ali Shah, Deloitte Pakistan**, *Good Corporate Governance: Essential to Prevent Conflicts of Interest and Fraud: Pakistan's Experience*, 13 (2004), https://www.oecd.org/site/adboecdanti-corruptioninitiative/39367990.pdf.

   "What Does Fraud Really Cost? To put it another way, each loss caused by internal or external fraud costs at least five times the original amount: One dollar in actual cash or property value is lost; A second dollar is spent identifying how the crime was committed; A third dollar is spent in identifying who committed the crime; A fourth dollar is spent prosecuting the person who committed the crime; and crime; and A fifth dollar is spent in suing the person who committed the crime for the recovery of the money taken."

7. **Brad Jones**, *Tackling Fraud Without the Friction*, BAI Banking Strategies (Feb. 10, 2016), https://www.bai.org/banking-strategies/article-detail/tackling-fraud-without-the-friction.

   "For much of its history, banking was a personal business, with customers interacting directly with their bankers and visiting bank branches when specific needs arose. In today's world, however, consumers expect full banking functionality online and on their mobile devices, which means the industry needs to find other ways to optimize the customer experience via multiple channels and devices.

   The problem is that the conservative personal history of banking has made it more difficult for the industry to adopt the latest technology. That's not to say the banking industry's concern around expanding functionality on these new platforms is unfounded. The faceless nature of mobile and online banking does present unique risks for financial transactions."

8. **Damian Handzy**, *New Models for Managing Risks*, Absolute Return & Alpha, WLNR 26483176 (Mar. 19, 2009).

   "New areas of research create a framework for understanding markets and risk management. The most interesting — and potentially promising — reaction to the current financial crisis has been the clamoring to fix, or even replace, one of the basic tenets underlying our understanding of economics, markets and risk management: the Efficient Market Hypothesis. The problems with the assumptions made by the EMH — which is the notion that market prices incorporate information instantaneously and rationally — have been well documented. But if markets don't have instantaneous access to perfectly correct information, if the behavior of all market participants is not totally rational and if price movements are not totally independent of all previous movements, then why use the EMH when it makes such obviously wrong assumptions? Regardless of how the answer is worded, it usually boils down to: 'Without these assumptions we couldn't do the math.'"

9. **David Divitt**, *Who Suffers the Most From False Positives?*, NCR: Fin. Blog (Nov. 19, 2015), https://www.ncr.com/company/blogs/financial/who-suffers-most-from-false-positives.

   "According to a new study from Javelin Strategy & Research, one in six (15 percent) of all cardholders experienced at least one false positive decline in the last year. Three times as many consumers are affected by a false positive as fraud, while the values involved are even more telling — $118 billion was incorrectly declined compared to $9 billion lost to fraud in 2014."

10. **Dean Nolan**, *Combating Fraud with Transaction Analytic*, BAI Banking Strategies (Apr. 2, 2014), https://www.bai.org/banking-strategies/article-detail/combating-fraud-with-transaction-analytics.

    "Transaction analytics, which enables financial institutions to analyze their customers' detailed transaction data over time to gain an understanding of customers' purchasing patterns and behaviors."

11. **Deloitte**, *Fraud Trends in the Banking Industry*, Wall St. J.: CIO J. (July 30, 2014), http://deloitte.wsj.com/cio/2014/07/30/fraud-trends-in-the-banking-industry/.

    "According to Prakash Santhana, a director in the Advanced Analytics practice for Deloitte Transactions and Business Analytics LLP, the battle banking and other sectors are waging against fraudsters is only becoming more pitched. 'Over the last 10 years, we've seen ever more sophistication in fraud schemes,' he says. 'There has been a significant increase in the number of

cyber criminal groups that are not just going after bank accounts, they are trying to get their hands on customer lists, personal identification data, and anything else that could be of economic value.'

Santhana says financial institutions are responding in a number of ways to the increase in credit/debit card fraud. Phishing fraud, he notes, is usually the primary approach cyber criminals use to 'take over' online accounts."

12. **Deloitte**, *The Latest Tools, Tactics for Battling Bank Fraud*, Wall St. J.: CIO J. (May 1, 2014), http://deloitte.wsj.com/cio/2014/05/01/the-latest-tools-tactics-for-battling-bank-fraud/.

"Advanced analytics holds tremendous promise for preventing and detecting fraud in the banking sector. This technology's ability to help identify suspicious patterns and anomalies hidden within ever-growing stores of transactional data could prove decisive in the sector's increasingly expensive battle against fraud. According to the American Bankers Association's 2013 Deposit Account Fraud Survey of member organizations, fraud against bank deposit accounts — including debit card, check, and online fraud — cost the industry $1.744 billion in losses in 2012.

Unfortunately, few banks are taking advantage of critical analytics capabilities. Although the financial services sector has pioneered many anti-fraud tactics with credit cards and other products, organizational siloes, outdated data management technologies, and turf battles between IT and anti-fraud groups have sometimes undermined important initiatives."

13. **Deloitte Canada**, *Tipping the Triangle Predictive Analytics to Mitigate Empty Envelope Fraud*, 1 (Apr. 2013), http://www2.deloitte.com/content/dam/Deloitte/us/Documents/deloitte-analytics/us-da-tippingthetriangle-020614.pdf.

"Focusing on that human element, the Fraud Triangle illustrates three key factors that enable individuals to commit fraud: pressure, opportunity and rationalization. The economic stress of the past few years has seen motive (or pressure) and opportunity on the rise. Motive arises from the financial pressure individuals feel when they confront personal challenges such as debt, addiction or greed; opportunity defines the way in which a person might inappropriately resolve their financial pressures, given a low perceived risk of detection. The final tenet of the triangle is rationalization, which sees an individual self-justifying the fraud act as necessary in order to silence his conscience."

14. *The Duty to Prevent Identity Theft Is Partly Shifting*, Communications Daily, WLNR 20499076 (Oct. 23, 2008).

"Tom Oscherwitz, vice president for government affairs and chief privacy officer at ID Analytics, said companies must also prepare for what happens after the deadline. Developing a policy isn't enough, he said. They must update policies and procedures periodically, and also think about how to put the rules into practice. ID Analytics performed a study of red flag hit rates and found 33 percent of 700,000 applications received in a 30-day period had an identity theft red flag. There will be lots of false positives, he said, and businesses must handle the red flag hits without slowing down operations to the point of alienating customers. Handling the flags identified in its study could cost between $347,000 and $1.5 million monthly, depending if they're handled interactively or manually, he said."

15. **Emil Eifrem**, *Battling Bank Fraud with Graph Databases*, BAI Banking Strategies (Apr. 12, 2016), https://www.bai.org/banking-strategies/article-detail/battling-bank-fraud-with-graph-databases.

    "While fraud is not completely preventable, there are approaches banks can take to significantly mitigate the growing issue, including focusing on relationships in banking data to uncover patterns of suspicious fraud activity. Traditional database technologies, while necessary for certain types of prevention, are not designed to detect the most elaborate fraud operations. In contrast, graph databases provide a unique ability to uncover a variety of important fraud patterns in real time, either in groups or on an individual basis, making them a powerful addition to any financial services firm's security arsenal."

16. *E-Verify: Preserving Jobs For American Workers: Hearing Before the Subcomm. on Immigration Policy and Enf't of the H. Comm. on the Judiciary*, 112th Cong., 150-51 (2011) (Richard M. Stana, Director, Homeland Security & Justice Issues, Government Accountability Office responds to question from Cal. Rep. Zoe Lofgren).

    "The false positives are at about 3-3.5 percent according to Westat, which means an individual is not authorized to work but somehow the system, either through identity theft or employer compliance with the individual getting a job inappropriately, identifies the individual as authorized to work.

    Now, when you throw around all these statistics, it is easy to get lost in the numbers. But when you start matching the number sets up — and it is hard to do because it is not exactly the same point in time and it is not exactly the same data set — but you start getting to the point where getting much further down on the false negatives is going to be very difficult to do. It is important to do it because you have people like you talked about, Ms. Lofgren, who are getting a bad shake out of the system. So you don't want to lose that intent, but it is getting tough because you were ratcheting this down into the below 2 percent range.

    The false positives — I don't know if we are ever going to get totally on top of that without having a better way to address the resource and enforcement question. It is not a matter of when or how. That is your call in what conjunction you do it. But that is the landscape here."

17. *E-Verify Progressing, But Still Needs Work, GAO Finds*, CQ Homeland Security, WLNR 1536911 (Jan. 20, 2011).

    "The federal electronic employment verification system known as E-Verify continues to whittle away at one of its opponents' primary criticisms — its error rate — but the U.S. Citizenship and Immigration Service still needs to make improvements to cut down on false positives and protect users against identity theft, according to the Government Accountability Office."

18. *False-positive Results Are Common with Cancer Screening*, CancerConnect.com (2016), http://news.cancerconnect.com/false-positive-results-are-common-with-cancer-screening/ (last visited Dec. 2, 2016).

    "The risk of obtaining a false-positive result from screening for prostate, lung, colorectal, and ovarian cancer is high and becomes cumulatively higher with ongoing screening — after 14 screening tests, the cumulative risk of a false-positive is 60.4 [percent] for men and 48.8 [percent] for women, according to the results of a study published in the Annals of Family Medicine."

19. **FICO**, *What Is the Future of Banking Fraud Management?: Changing Market Forces Require a New Approach to Enterprise Fraud Management,* 2 (Aug. 2012), http://www.fico.com/en/wp-content/secure_upload/62_Future_of_Banking_Fraud_Management_2896WP.pdf.

"The potential for losses is certainly considerable. As always, fraudsters are shifting their attentions from more defended to less defended targets, and today there are plenty of fresh opportunities. New online and mobile services open up vulnerabilities fraudsters are quick to exploit. Under time-to-market pressure, banks may launch without adequate defenses. Indeed, the newness of the services, and the unknowns about how fraudulent and legitimate users will behave, make it difficult to extend protection with traditional fraud detection methods alone."

20. *The Fight Against Tax Crime: Our Focus: Refund Fraud*, Austl. Taxation Office, https://www.ato.gov.au/general/the-fight-against-tax-crime/our-focus/refund-fraud/ (last modified Aug. 3, 2015).

"Refund fraud occurs when people dishonestly claim refunds, rebates or offsets they aren't entitled to. This can happen in a range of ways, from claiming fictitious expenses to creating false documentation to support a claim. Some individuals lodge fraudulent claims in their own name or for their business; others lodge a claim on behalf of another person. Identity crime related to refund fraud is an increasing problem, with stolen identities used to lodge false income tax returns and activity statements with the aim of fraudulently getting refunds."

21. *Fraud Losses and False Positives: The Numbers*, SecuredTouch (Dec. 2015).

"Companies want to avoid fraud. They also want to avoid false positives. In total, around 33 million adults in the United States are wrongly blocked each year from completing a purchase with a credit card. That's around 15% of cardholders! The total of these blocked sales amounts to $118 billion, while the cost of real card fraud only amounts to $9 billion. This shows false positives cost businesses more than the actual fraud."

22. **Fraud Prevention Expert Grp.**, European Comm'n, *Report on Identity Theft/Fraud*, (Oct. 22, 2007), http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf.

"In some EU Member States identity theft/fraud is the fastest growing type of financial fraud." (at 2).

"The misuse of personal data to impersonate somebody else and abuse of his/her banking/financial services facilities is a growing concern in developed societies." (at 5).

"Identity Theft occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead."

"Identity Fraud occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of identity fraud." (at 7).

"In Sweden, where personal tax data is public, the agency in charge has specific controls that allow consumers to alert the authorities to abuse of their data, and thus minimise the on-going impact of such an abuse." (at 24).

"Identity theft/fraud does not only affect the financial sector. Its effects go beyond … Technology is part of the solution but will not be the only solution." (at 37).

23. **Georgios L. Vousinas**, *The Critical Role of Internal Auditing in Addressing Bank Fraud: A Conceptual Framework*, 5 Case Stud. J., 67 (2016).

"The recent global financial recession highlighted the critical role that the banking system plays in the modern economy. Banks are complex financial institutions that operate in a constantly changing business environment and deal with high levels of risk, while facing fraudulent actions in regular basis. In order to address these problems, banks engage in various internal audit techniques such as the implementation of controls and prevention tools, the usage of anti-fraud methods and data mining. The aim of this paper is to highlight the crucial role of internal auditing in addressing bank fraud. This is achieved by initially providing a review of both theoretical and empirical literature which helps in determining the value of internal auditing and then by proposing a conceptual framework in order to justify its interconnection with bank fraud, and also to serve as a guide for all future reference. The results confirm the fact that internal audit can play a major role in risk assurance and bank fraud management thus, ensuring banks' normal and uninterrupted operation. The paper also provides some useful insights for future application of internal audit methods thus, laying the ground for a fruitful dialogue among the various stakeholders."

24. **Graeme Burton**, *Connecting the Dots at HMRC,* Computing.co.uk (Feb. 21, 2013), http://www.computing.co.uk/ctg/feature-/2244719/connecting-the-dots-at-hmrc.

"It is, though, looking to bring in contractors with deeper skills in specialist areas such as predictive analytics, and experience in the commercial banking and insurance sector to provide extra depth in terms of thinking about the data and modelling approaches.

'It's a similar kind of market. They are trying to risk assess individuals for giving people loans. And we are in the business of risk assessing people based on information around their tax affairs. They are very similar kinds of activities,' says [Mike] Hainey [Head of the risk and intelligence service data analytics team at HMRC]."

25. **Gregg S. Henzel, Troy La Huis & Thomas M. Paar**, Crowe Horwath, *Using Model Calibration and Optimization to Reduce Fraud Risk: How Financial Institutions Can Identify Fraud More Effectively While Reducing Costs*, 3-4 (2015), https://www.crowehorwath.com/folio-pdf/Using-Model-Calibration-and-Optimization-to-Reduce-Fraud-Risk-Article-RISK-16007-008A.pdf.

"High false-positive rates present two challenges to organizations. The first is cost: As rates rise, fraud prevention requires more labor and becomes more expensive. Indeed, at very high rates, prevention becomes so costly that — from a purely economic view — it could be cheaper simply to let fraud occur.

The second problem with high false-positive results is how it affects the engagement level of those analyzing the company's data for evidence of fraud. When rates start to climb above 25:1, analysts know their next alert is unlikely to reveal fraud. Their incentive to remain diligent declines; their minds wander, and morale erodes. In contrast, when false-positives run 5:1, analysts know that they are just moments away from potentially uncovering another instance of fraud. They're engaged, focused, and efficient."

26. **Guardian Analytics**, *Best Practices for Detecting Banking Fraud*, 2 (2013), http://docs.bankinfosecurity.com/files/whitepapers/pdf/708_Best_Practices_for_Detecting_Fraud_white_paper.pdf.

"Look for inconsistencies with previously demonstrated 'normal' behavior — This is called 'anomaly detection,' which is a well-established, analytical technique for identifying unexpected or unusual behavior relative to previously established patterns of normal behavior … In order to commit banking fraud, cyber criminals must at some point access the online banking account to gather information, set up an attack or initiate a fraudulent transaction, and when they do, they will do something that is unusual or unexpected in the context of your real client's typical banking behavior. The power of using anomaly detection lies in the fact that it doesn't matter how the account is compromised — whether it's a Trojan or other malware, stolen credentials, or social engineering through customer service - the suspicious behavior relative to established norms is what provides a clue or signal that something is amiss … Use layered security — there is no silver bullet when it comes to fraud prevention. Whether it's device, ID, tokens, out of wallet challenge questions, out of band authentication, or positive pay, fraudsters have found a way to get past each of them. But it is extremely difficult to get past ALL of them. A layered security strategy, as called for by the FFIEC, means that when (not *if*, but *when*), the fraudster gets past one layer, another confronts them. Each layer adds to the effectiveness of the entire security strategy."

27. **Guardian Analytics**, *Guardian Analytics Prevents Online Fraud From Login to Logout With FraudMAP Version 2.0*, PR Newswire: News (Aug.18, 2008), http://www.prnewswire.com/news-releases/guardian-analytics-prevents-online-fraud-from-login-to-logout-with-fraudmap-version-20-64911422.html.

"The newly advanced activity modeling capabilities in Guardian Analytics' FraudMAP 2.0 analyzes all online account activity within and across sessions, including seemingly benign actions such as viewing check images or updating contact information. Sophisticated algorithms predict and weigh inherent risk by a number of parameters, such as expected account holder behavior and size of potential loss, to more accurately alert financial institutions to suspicious activity while minimizing false positives. In addition, FraudMAP 2.0 provides banks, credit unions, and brokerages with extensive session and customer-specific context for advanced fraud and identity theft investigation and prevention."

28. **IBM Software**, *Fighting Fraud in Banking with Big Data and Analytics*, 2 (2014), http://www-07.ibm.com/au/pdf/Fighting_Fraud_in_Banking_with_Analytics.pdf.

"Fraud and financial crime can no longer be an acceptable cost of doing business. Fraud schemes are growing more sophisticated, the costs are getting higher and customer expectations are ever-increasing. In addition to triggering financial losses, fraud drives significant investigative and legal costs, erodes consumer confidence and devastates brand image. To meet these challenges, the banking industry is fighting fraud in new ways using big data and analytics capabilities."

29. **Inspector-Gen. of Taxation**, Austl. Gov't, *Review into the Australian Taxation Office's Compliance Approach to Individual Taxpayers - Income Tax Refund Integrity Program*, at vii, 21 (2013), http://igt.gov.au/files/2014/11/income-tax-refund-integrity-program.pdf.

"The Inspector-General of Taxation's (IGT) review into the ATO's [Australian Taxation Office's] income tax refund integrity program (ITRIP) is one of three concurrent reviews examining aspects

of the ATO's compliance approach to individual taxpayers. The ITRIP comprises a series of analytical models designed to detect instances of overclaimed deductions, offsets or other credits in income tax returns. The ATO stops these returns for manual review before any refunds are issued to the taxpayer.

The review arose out of taxpayer and tax agent concerns regarding extended ATO delays in processing income tax returns held for review under the ITRIP. Significant complaints were raised with the Commonwealth Ombudsman, the ATO's Complaints section and the IGT in 2011-12 when higher than expected numbers of tax returns were held (109,000 returns were held when only 33,000 had been expected) leading to extended delays in the processing of those returns. This was exacerbated by the inability of taxpayers or tax agents to ascertain specific reasons for such delays or to have their returns expedited. Moreover, it was contended that the ATO's communication led to the perception that the ATO considered these taxpayers to be dishonest or fraudulent." … "EFFECTIVENESS OF THE ITRIP MODELS ITRIP strike rates [2.14] A strike rate is one means of assessing the effectiveness of a particular approach or strategy. A strike rate may generally be defined as the proportion of selected taxpayer cases, in which the relevant risk was confirmed resulting in a positive outcome or action, measured against the total population. Those taxpayers incorrectly selected or whose tax returns were released without action are not included and are considered to be false positives in the risk identification process."

30. **Inst. Internal Auditors *et al.***, *Managing the Business Risk of Fraud: A Practical Guide*, 34 (June 2008), http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf.

"Organizations can never eliminate the risk of fraud entirely. There are always people who are motivated to commit fraud, and an opportunity can arise for someone in any organization to override a control or collude with others to do so. Therefore, detection techniques should be flexible, adaptable, and continuously changing to meet the various changes in risk."

31. *The IRS Data Breach: Steps to Protect Americans' Personal Information: Hearing Before the S. Comm. on Homeland Sec. & Gov't Affairs*, 114th Cong. 10 (June 2, 2015) (statement of Kevin Fu, Associate Professor, Department of Electrical Engineering and Computer Science, University of Michigan), http://www.hsgac.senate.gov/hearings/the-irs-data-breach-steps-to-protect-americans-personal-information.

"The IRS used instant knowledge-based authentication in an attempt to verify identities seeking transcripts of tax returns. Unfortunately, the threat landscape is changing quickly as attackers adapt to newly fortified defenses. There will always be fraud, but a reasonable goal is to make it difficult for a single adversary to commit wide-scale, automated fraud. A major challenge in identity theft prevention is maintaining low false-positives (that would deny legitimate requests) and low false-negatives (that would allow identity theft) while serving the technologically diverse, tax paying U.S. population."

32. **Jason Freeman**, *One Step Forward and Two Steps Back: Identity Theft and Taxes*, AICPA.ORG, (July 24, 2015), http://www.aicpa.org/interestareas/tax/newsandpublications/taxsectionnews/2015/pages/072415_issuespotlight.aspx.

"Tax-related identity theft is a complex and evolving threat — and one that costs taxpayers billions of dollars annually. It is, without question, one of the most pressing challenges that we face in the

world of tax administration. And while the government has taken some steps forward over the past several years in the effort to stop tax-related identity theft, it has also suffered some major setbacks. The current data indicates that the threat is growing, not shrinking, and without a more effective deterrence model, that trend is likely to continue in the wrong direction."

33. **Jayaprakash Nair**, *Analytics Applied — Fraud Prevention and Detection in the Banking Sector*, Aspire Sys. (Mar. 28, 2016), http://blog.aspiresys.com/-digital/big-data-analytics/analytics-applied-fraud-prevention-and-detection-in-the-banking-sector/.

"In a recent survey conducted by Deloitte on the Banking industry, 93% of the respondents indicated that fraud has grown in the last 2 years. Apart from the financial losses, these incidents leave a dent in the banks' reputation … Majority of the frauds happened due to either human negligence or malpractice. Part of the solution obviously is to train the staff better, tighten the manual processes, and increase the audits — in general, increase the sense of responsibility and ownership. But while those steps are definitely necessary, they are not sufficient. A large part of the solution is to use automated checks and balances throughout the workflow to ensure that such activities are either prevented before they occur, or at least caught and corrected at the time of occurrence.

… Only about 26% were caught at the point of transaction (10%) or with an automated system (16%). Agreed that these statistics are based on a sample of the population and are approximate. But even after allowing for such a sampling error, it is clear that there is a huge opportunity for the banks to reduce their losses, both tangible as well as intangible. In fact, the intangible losses — loss of goodwill, loss of confidence/faith in the bank etc. — could lead to much deeper and long-term losses for the bank's brand image and bottom line, especially in the wake of disruptive Fintech innovations knocking on the consumer's doors."

34. **Keith Mueller**, *How Technology is Shaping the Fight Against Fraud*, Inc.com (Feb. 25, 2015), http://www.inc.com/keith-mueller/technology-shaping-the-fight-of-fraud-in-2015.html.

"To minimize the potential damage of fraud, companies need to invest not just in more advanced technology but in people and policies for detecting attacks as quickly as possible. While the networks are just too large to prevent every attack from occurring, detection is crucial. Most companies do not have adequate protocols and staff in place to deal with incidents of fraud. While advanced technology serves as a great tool to combat fraud, the issue should be viewed as more than just an IT problem and looked at as a business problem. Here are some steps to take:

- Put a clear focus on segregation of duties (spread and rotate financial responsibilities, control who views sensitive documents)
- Offer internal and external audits (monthly profit and loss reviews, monthly balance sheet reviews)
- Develop protocols for electronic banking transactions (*e.g.*, limiting access, verbally confirming requests, two-step authentication process, safeguard data)."

"By taking these actions, companies can begin building a culture of system-wide accountability rooted in honesty, integrity, and transparency. Remember, the cost of trying to prevent fraud is far less expensive to a business than the cost of fraud committed on a business."

35. **Madan Lal Bhasin**, *Combatting Bank Frauds by Integration of Technology: Experience of a Developing Country*, Insight Med. Pub. (Mar. 28, 2016), http://www.imedpub.com/articles/combatting-bank-frauds-by-integration-of-technology-experience-of-a-developing-country.pdf.

"Fraud is a worldwide phenomenon that affects all continents and all sectors of the economy. With the rapidly growing banking industry in India, frauds are increasing fast, and fraudsters have started using innovative methods. Shockingly, the banking industry in India dubs rising fraud as an inevitable cost of business. One of the most challenging aspects in the Indian banking sector is to make banking transactions free from electronic crime. There is no "one silver bullet" to stop all frauds forever. By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud. Behavioral analytics monitor navigation techniques and other aspects of a user's online behavior to search for anomalies or suspicious activity. Behavioral Analytics: This is helping businesses identify enemies disguised as customers. The data analytics implemented by the institutions to understand customer behavior, preferences, etc. are also helping in the detection of fraudulent activity either in real-time or post mortem."

36. **Martin Merzer**, *Poll: As Card Fraud Rises, So Do False Alarms*, CreditCards.com (June 16, 2014), http://www.creditcards.com/credit-card-news/poll-fraud-false_alarm-block-transactions-1276.php.

"Millions of U.S. credit card users are experiencing — and generally tolerating — transactions being blocked or questioned as credit card companies fortify fraud-blocking systems in response to an epidemic of data breaches and credit scams, according to a new survey released Monday by CreditCards.com. The survey found that nearly four out of 10 frequent credit card users have experienced a credit card fraud alert — a transaction blocked or questioned by their credit card company because the purchase triggered a fraud alert. Two out of three affected credit card users said that some or all of the blocked or questioned transactions were actually legitimate purchases."

37. **Mary Shacklett**, *Fighting Tax Fraud with Analytics*, TechRepublic.com (Apr. 14, 2016), http://www.techrepublic.com/article/fighting-tax-return-fraud-with-analytics/.

"The Maryland Comptroller Office is one example of the efforts that states are making to improve fraud detection through the use of analytics … The state's new process, fueled by analytics, now uncovers fraudulent returns at a rate of 50 to 60% before the returns are even manually reviewed to confirm the findings."

38. **Matthieu Aikins**, *Doctors With Enemies: Did Afghan Forces Target the M.S.F. Hospital?,* The N.Y. Times, (May 17, 2016), http://www.nytimes.com/2016/05/22/magazine/doctors-with-enemies-did-afghan-forces-target-the-msf-hospital.html?_r=0.

"Restricted to a supposedly noncombat role as advisers, the Special Forces in Kunduz ended up calling in the airstrike, which was in support of Afghan troops against a target a quarter-mile away, as self-defense, which meant that it bypassed many safeguards intended to prevent civilian casualties."

39. **National Audit Office**, Her Majesty's Revenue & Customs (HMRC), *Tackling Tax Fraud: How HMRC Responds to Tax Evasion, The Hidden Economy and Criminal Attacks*, 20 (2015), https://www.nao.org.uk/report/tackling-tax-fraud-how-hmrc-responds-to-tax-evasion-the-hidden-economy-and-criminal-attacks/.

"Revising its Strategy (2013 to 2014) HMRC began to develop a long-term strategy for its work. It aims to tackle the behaviour that leads to non-compliance, which should lead to more people giving HMRC correct information. This will allow HMRC to focus on the dishonest minority. This strategy is based on the three broad things a tax administration can do: create the right environment for people to pay their taxes (HMRC refers to this as 'promote'); put systems in place to identify and stop tax fraud as taxpayers give HMRC information ('prevent'); and identify tax fraud and take action in response ('respond')."

40. **Neta C. Crawford**, *Targeting Civilians and U.S. Strategic Bombing Norms: Plus* ça *Change Plus C'est la Même Chose, in* The American Way of Bombing: Changing Ethical and Legal Norms, from Flying Fortresses to Drones 64, 81 (Matthew Evangelista & Henry Shue, eds., 2014).

"First, algorithms that estimate noncombatant killing for preplanned strikes were employed much more widely than in previous conflicts. These algorithms are a set of decision rules, formulas, and inputs used to calculate risk and likely harm to noncombatants. And second, there was a threshold of risk to noncombatants that was considered acceptable given the understanding of military necessity and the estimated risk to U.S. forces."

41. **Oracle**, *Reducing False Positives Without Increasing Regulatory Risk*, 1 (2011), http://www.oracle.com/technetwork/middleware/ows/documentation/ows-reducing-false-positives-wp-1864957.pdf.

"False positives are the scourge of the Money Laundering Reporting Officer (MLRO) — the person responsible for protecting the reputation and security of a financial institution. Every occurrence of a client record matching a name on a sanction, risk, or PEP (politically exposed persons) register has to be investigated, and yet the review and research of false positives costs institutions time and manual effort. 'Fuzzy' techniques are essential to finding inexact matches, but they often produce large numbers of records for review, and the vast majority of these will be false positives.

With some institutions swamped by the volume of false positives, the temptation to tighten match rules can be irresistible. Although this might reduce the immediate pain of so many false positives, it often increases the probability of a more insidious risk — that of false negatives. False positives do cost time and effort, but false negatives allow criminals access to the financial system and can result in fines for both the institution and the individual MLRO — and a loss of commercial reputation as well. This white paper examines some of the common matching techniques and advises MLROs that, rather than having to choose one from among an array of techniques that are imperfect in themselves, they can implement a broad array of technologies now incorporated in today's most effective watchlist screening solutions."

42. *Organisations Pay the Price of Chasing False Alerts*, ITWeb (S. Afr.), WLNR 7507843 (Mar. 10, 2016).

"Organisations spend too much time investigating false alerts, resulting in undetected serious malware threats, says Forcepoint's Neil Thacker. The average company spends almost 199 hours a week investigating malware infections on their computer systems. Another 230 hours a week is spent on cleaning or fixing the organisation's infected devices. With all this time spent

on investigations, there are still around 40% of infections that go undetected in an average organisation's network operating system. This is according Neil Thacker, information security and strategy officer at Forcepoint EMEA, who was speaking at the Forcepoint security briefing forum organised by IT Web last week. Thacker said this is a significant amount of time for any company to spend on investigating false positive alerts and chasing erroneous cyber alerts such as suspected malware and viruses that turn out to be nothing more than dead ends."

43. *Patent Application Titled "System and Method for Mobile Identity Protection of a User of Multiple Computer Applications, Networks or Devices Using a Wireless Device,"* Telecomm. Wkly., WLNR 4754242 (Feb. 26, 2014).

"Credit card issuers and financial institutions, such as banks, attempt to limit financial identity theft and fraud losses by analyzing a variety of data and information associated with, for example, an automated credit card transaction. Rules-based 'parameter analysis' is used along with pattern recognition and probabilistic techniques to determine the legitimacy of a card transaction. Parameter analysis techniques are used to examine, for example, the number of credit card transactions on a particular account within a specified period of time, say 24 hours, and the dollar amount of the transaction. If the number of transactions or the dollar amounts exceed some pre-defined threshold, the transaction can be flagged as potentially fraudulent and further action can be taken. This action may be as drastic as denying the transaction and blocking the card holder's account. Parameter analysis, however, often times yields false-positive results, where the financial transaction is in fact legitimate, but falls outside the parameter thresholds set."

44. **PricewaterhouseCoopers (PwC)**, *Financial Services Sector Analysis of PwC's 2014 Global Economic Crime Survey: Threats to the Financial Services Sector*, 4 (2014).

"The Financial Services ("FS") sector results from PwC's seventh Global Economic Crime Survey are the most comprehensive and intriguing to date. There were 1,330 responses from the FS sector alone — 26% of the 5,128 responses received from all sectors. FS respondents hailed from 79 different countries — making this FS sector report truly global and representative of views on economic crime in its many guises, from fraud and cybercrime to money laundering and bribery and corruption.

Our survey questions were designed to assess corporate attitudes to economic crime in the current economic environment, the types of fraud encountered during the survey period, whether cybercrime is becoming more prevalent, and the extent of bribery and corruption, money laundering and anti-competition experienced."

45. **Rajesh Ramachandran**, Cognizant, *OFAC Name Matching and False-Positive Reduction Techniques*, 1 (2014), https://www.cognizant.com/InsightsWhitepapers/OFAC-Name-Matching-and-False-Positive-Reduction-Techniques-codex1016.pdf.

"Financial institutions typically spend more time, money and resources investigating false positives as transaction volume and money transfer activity increases. This can be reduced by improving their OFAC [Office of Foreign Assets Control] compliance processes and implementing new software with sophisticated time-saving matching algorithms that recognizes different variants or misspellings of names and thus reduces the number of false positives to a minimum. Other approaches include intelligent automation workflows, robust management and audit controls, implementing industry best practices and gaining the technical ability to analyze past sanctions screening results. This

white paper offers advice on unique strategies to reduce the false-positive rate, including name-matching techniques and critical mitigation steps."

46. *Recovering £7 Billion in Additional Tax Revenues*, SAS, http://www.sas.com/en_gb/customers/hm-revenue-and-customs.html (last visited Oct. 21, 2016).

"The outcome of HMRC's analytics and the Connect system — working faster and smarter, improving detection rates and finding new opportunities for prevention and deterrence — will see the government avoid significant financial losses and instead receive higher tax revenues.

'We're saving time — for example, we can limit false positive results and avoid wasted interventions,' says Cockerill. 'The more we know about people, the more opportunities we have to deselect them. Risks that can seem really strong are explained when you can look at networks and have far richer data to work with. That broader picture means we can ease burdens on taxpayers. We're also moving into an era of larger data sets that we want to analyze using our toolkit: tables approaching billions of rows in size. In many ways this is becoming much more about 'heavy lifting' to get the data in shape.'"

47. *Researchers Submit Patent Application, "Method and System for Determining and Assessing Geolocation Proximity," for Approval*, Computer, Networks & Commc'n, WLNR 25463486 (Sept. 3, 2015).

"... many existing fraud detection and prevention technologies can and do provide a false positive indication of fraudulent activity. Besides the fraud detection and prevention mechanisms already mentioned, other technologies may be employed such as behavioral profiling that is used to detect anomalous behavior. These technologies employ intelligent algorithms to analyze past user behavior when a user attempts to engage in some activity or transaction that is similar to a previous activity or transaction. If the individual's behavior when engaging in a secure activity is not consistent with that individual's past behavior, a likelihood of fraudulent activity may be deduced."

48. **RSA Security, Inc.**, *Barclays Bank Protects Online Banking Users with Behind-the-Scenes Authentication Using RSA Cyota Transaction Monitoring*, PR Newswire (Mar. 22, 2006), http://www.prnewswire.com/news-releases/barclays-bank-protects-online-banking-users-with-behind-the-scenes-authentication-using-rsar-cyotar-transaction-monitoring-55494512.html.

"RSA Cyota Transaction Monitoring provides strong, reliable protection against online fraud by analysing and scoring all online banking transactions in real-time. The bank can then decide how to handle high-risk transactions, including blocking the transaction or conducting a manual review and seeking further identification of the user. The system, which provides a second factor of transparent authentication using IP address, user and device profiles, incurs no change in the user experience. Additionally, the Company's risk-based, one-time password and EMV authentication solutions can be deployed — via RSA Adaptive Authentication — on top of Transaction Monitoring to provide the additional transaction validation, should it be required.

The RSA Cyota risk engine compares each online transaction to an automatically generated profile of that user's known behavior and other criteria, such as digital fingerprints, geographic location, device information and more. The solution also compares the data to known fraud patterns compiled by the RSA Cyota eFraudNetwork™ community, the world's most effective online financial fraud network. With membership comprising thousands of financial institutions worldwide, including the United Kingdom's largest banks, the eFraudNetwork collates some of the

best, most up-to-date intelligence from across the globe, giving banks instantaneous information and immediate protection."

49. *The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, a Drain on the Public Treasury: Hearing Before the Subcomm. on Fiscal Responsibility and Econ. Growth of the S. Comm. on Fin.*, 112th Cong., 65, 75-76 (2011) (statement of James R. White, Director Strategic Issues, U.S. Government Accountability Office).

"Beyond screening returns with known tax-related identity theft issues, screening all tax returns for possible refund fraud would pose similar trade-offs, but on a grander scale. For example, as noted above, one way to check for identity theft is to look for significant differences between current year and prior year tax returns, but this could be confounded by a large number of false positives. IRS officials told us that in 2009 there were 10 million address changes, 46 million changes in employer, and millions of deaths and births. Checking all returns that reflect these changes for possible refund fraud could overwhelm IRS`s capacity to issue refunds to legitimate taxpayers in a timely manner."

50. **Tom Johnson**, *Real-Time Fraud Detection: The Holy Grail for Fin. Institutions,* PAYMENTSSOURCE, WLNR 9344832 (May 11, 2011).

"As part of (the) payment approval process, financial institutions need the tools to create their own scores and the ability to integrate their own data with additional sources to determine whether a transaction is fraudulent. Many banks currently decline specific transactions based solely on their own data. Looking at external data sources can help banks see that someone has just declared bankruptcy or reported identity theft. Also, segmenting people based on a cardholder's behavior helps identify what is likely a stolen identity or fraud."

51. *The Transportation Security Administration's Aviation Passenger Prescreening Programs: Secure Flight and Registered Traveler: Hearing Before the S. Comm. on Commerce, Science, & Transp.*, 109th Cong., 11,14-15 (2006) (statement of Cathleen A. Berrick, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office).

"According to a TSC [Terrorist Screening Center] official, TSA [Transportation Security Administration] and TSC plan to enter into a letter of agreement that will describe the data elements from the terrorist-screening database, among other things, to be used for Secure Flight. To address accuracy, TSA and TSC plan to work together to identify false positives — passengers inappropriately matched against data contained in the terrorist-screening database — by using intelligence analysts to monitor the accuracy of data matches. An additional factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system`s inability to identify passengers who assume the identity of another individual by committing identity theft, or who use false identifying information. Secure Flight is neither intended to nor designed to address these vulnerabilities."

52. *Transportation Security Administration's Office of Intelligence: Progress and Challenges: Hearing Before the Subcomm. on Intelligence, Info. Sharing, & Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 109th Cong., 32, 45-46 (2006) (statement of Cathleen A. Berrick, Director, Homeland Security and Justice, U.S. Government Accountability Office).

"Prior to its rebaselining effort, TSA had also reported that it planned to work with TSC to identify false positives as passenger data are matched against data in the TSDB, and to resolve mistakes

to the extent possible before inconveniencing passengers. The agencies were to use intelligence analysts during the actual matching of passenger data to data contained in the TSDB to increase the accuracy of data matches. When TSA`s name-matching technologies indicated a possible match, TSA analysts were to manually review all of the passenger data and other information to determine if the passenger could be ruled out as a match to the TSDB. If a TSA analyst could not rule out a possible match, the record would be forwarded to a TSC analyst to conduct a further review using additional information. Until TSA completes its rebaselining effort, it is uncertain whether this or another process will be used to help mitigate the misidentification of passengers. An additional factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system`s inability to identify passengers who assume the identity of another individual by committing identity theft, or who use false identifying information. Secure Flight was neither intended nor designed to address these vulnerabilities."

53. **TrustedID**, *TrustedID™ Launches New Threat Score™ Identity Theft Risk Rating Service*, PR Newswire (Oct. 27, 2009), http://www.prnewswire.com/news-releases/trustedidtm-launches-new-threat-scoretm-identity-theft-risk-rating-service-66376852.html.

"Identity Threat Score with IdentityScan empowers consumers with access to the type of sophisticated technology that is currently used by major credit card providers around the globe to analyze risk. The system works by identifying specific patterns and combinations of information proven to increase a consumer's risk of identity theft. By analyzing this data, IdentityScan is able to accurately predict the likelihood of identity theft, while limiting the number of false positive alerts that lead to unnecessary concern for consumers."

54. **Udi Solomon**, *The Only Thing Worse than False Positives Is No Positives!*, ThetaRay (June 23, 2015), http://www.thetaray.com/the-only-thing-worse-than-false-positives-is-no-positives/.

"Originally termed by the medical world, false positives are no laughing matter. Of course, in the financial sector, we're not talking life or death, but don't underestimate the damage false positives can cause. Credit card fraud for example is estimated to bring losses of up to $190 billion annually. Nevertheless, false positives can mean significant losses to revenue, reputation and customer relations.

Being on the customer end of a false positive is not much fun either, whether rejected for a loan or inexplicable credit card blocks at the point of payment. From the business side, fraud alerts have to be managed somehow, they can't be ignored for fear of missing the genuine instance of crime. Someone has to pick up the bill for lending fraud and the buck stops with the issuing bank."

55. **Written Statement of Jeffrey A. Porter**, On Behalf of the American Institute of Certified Public Accountants, presented to the Internal Revenue Service Oversight Board, *Public Forum Panel 2: Working Together to Combat Fraud* 7 (2013).

"The IRS [Internal Revenue Service] has made great strides in issuing IP PINs [Identity Protection Personal Identification Numbers] to 250,000 taxpayers victimized by identity theft in 2012, with approximately 770,000 issued during the 2013 filing season. However, we believe the IRS could issue many more IP PINs and aid even more identity theft victims.

New technological developments may contribute greatly to a reduction in the Service's cycle time for addressing identity theft cases. Technology improvements should also focus on providing the IRS with an ability to conduct a global account review for an identity theft victim by identifying prior returns that have been impacted and subject to potential examination and collection actions."