ISSN: 2054-7404
Archives of Business Research; Vol. 14 No. 03 (2026) (13-23)
https://doi.org/10.14738/abr.1403.20109

AI - Massive Data Management Conducive to Optimal VAR Model Making

Reza G. Hamzaee, PhD & Maryam Salimi, PhD

1. BOG-Distinguished Professor Emeritus of Economics, Missouri Western State University, St. Joseph, MO, 64507, USA and Owner/Chair: 1) RMD Hamzaee Econometrics International Consultants LLC, and 2) RMH Econometrics – Bus Management Consultants, Inc., Overland Park, USA
2. University Instructor of Infographics, Mass Media, and Data Processing Management, Tehran, Iran

Abstract: While a comparative review of some selected applicable and controversial aspects of AI is presented in addressing both academic and operational concerns, respecting the supremacy of credible data, the data massiveness, and the significance of varying essential facts, instead of hypothesizing a predetermined economic or any other scientific models, we are proposing a data-based Vector Autoregression (VAR) methodology for AI optimal application to the ongoing fraud and anti-fraud structure and hence, more effective policymaking. It may include many other macro or microeconomic policy optimization. Hopefully, the entire attempt will portend some tangible prospective contribution in an achievable positive societal change. Our adopted data will be compiled in a broad international and national similarly surveyed source by Dorris (2022) and/or various governmental fraud data sources.

Keywords: Anti-Fraud Policy, Artificial Intelligence, Massive Data, VAR Modeling

INTRODUCTION

While AI has attracted considerable global attention, it has primarily been identified as another challenging, as well as controversial, phenomenon, reflecting a contrasting integration of astounding, good, bad, and ugly for good reasons all along. AI has proven to make so many contributions in marketing, management, data compilation and implementation, business and government policymaking, intelligence and security industries, tax-related concerns and monitoring, etc.

Yet it is impossible at this point of time to ignore the drastic and excessive potential and actual damage that AI has caused in daily lives of people through invasion of their deserving peace and privacy rights, and even worse to be subjected to AI-driven fraud and crime. It has unfortunately been quite a trend to fake news, data, pictures, video images, bank accounts of individuals in order to acquire ransom and or defeat political candidates. The ongoing diminishing ethical and cultural values through the destructively expanding fraud in both business and politics, have appeared to be even worse under speedy impacts of AI abusers around the world. “Facts versus alternative facts” are being more of the commonly penetrating culture and communication, altogether conducive to shattering the public trust in establishments, including governments, business corporations, politicians, religiosity, and ultimately, what is right or wrong.

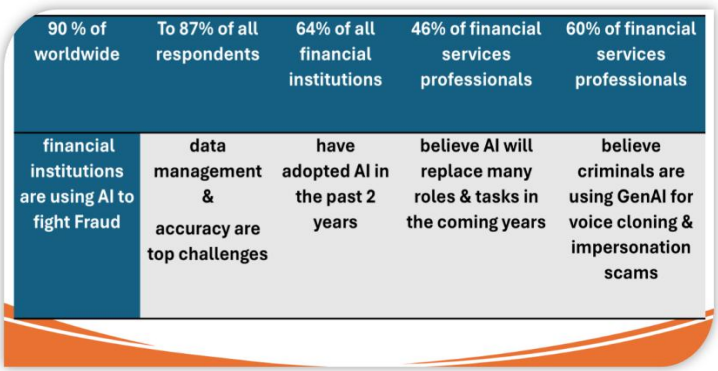
AI-KNOWLEDGE FLOW

Artificial Intelligence: A Tale of Amazement, Good, Bad, and Ugly

Benedict Jun Ma and Maria Jesus Saenz (Fall 2025) portend that, given limitations in each robot and humans, AI would contribute to making each more capable to enhance their integrated shares. When human capability is essential and robot lacks autonomy, various published research has supported their conclusions that AI can boost their collective performance.

An Oracle NetSuite-sponsored short piece, authored by Ashok Manthena (2025), "CFO's AI Survival Guide Skills You Need Now," offers a road map for business survival in 5 significant components, including "Deep Industry Expertise, Mastery of Core Finance Processes, Basic Coding Skills, Data Visualization, and Data Science Acumen Companies." Yet Anderson, Parker, and Tan (Fall 2025) stressed the inadvertent growing debt because of careless deployment of AI and a lack of appropriate coding productivity. Isik and Goswami (Winter 2026), suggest that there are three obstacles impeding responsible AI deployment: accountability, strategy, and resource gaps. In their Winter 2026 MIT Sloan Management Review, they provided an expansive approach to close each of those three gaps. Dyck, A. et el. (2013, February 22) focused on the pervasiveness of corporate fraud, and Embroker (2023, June 6) analyzed the employee theft issues.

Table 1: The Recent AI Survey Results



Source: Feedzai: 2025 AI Trends in Fraud and Financial Crime Prevention (reformatted and tabulated by the authors)

Table 2: Types of Financial Institutions

Retail Banks	Acquiring Banks	Commercial Banks	Investment Banks	Credit Unions or Building Societies	Fintech/Digital Banks
22%	18%	18%	16%	12%	12%

Source: Feedzai: 2025 AI Trends in Fraud and Financial Crime Prevention (reformatted and tabulated by the authors)

As reported by DataWalk (2025), Sue Gordon, the former Principal Deputy Director at the U.S. National Intelligence warned that: "I don't think there's any way that we get to a future that is cyber secure without both the public and private entities coming

together to find some solutions." One of the examples of anti-fraud cases which are designated to reduce fraud losses and identify potential crime rings automatically and other suspicious practices, DataWalk is one of the providers of robust data analytics platform. The following cases are pursued:

- **AML (Anti-Money Laundering)**, boosting ongoing compliance efficiency, while protecting clients' investment in existing AML tools.
- **Cryptocurrency Investigations**, investigating bad actors through massive data software integrating clients' data through blockchain technology with other relevant key data sources.
- **Intelligence Analysis**, using massive data solutions to quickly generate actionable intelligence from vast amounts of disparate data across numerous sources.

Furthermore, Statista (2023) highlighted the tax evasion fraud, which is always too costly to any nation.

Additionally, DataWalk (2025) has provided a series of analytical research pieces, which are most topical in today's AI-related applicable studies, such as corporate and financial reports detailing revenue, contract values, and strategic business insights. Other analytic issues involving white papers, case studies on fraud detection, anti-money-laundering, and investigative processes, platform users and potential clients, an integrative perspective on enterprise analytics, investigative intelligence, and subscription-based software adoption during 2025. DataWalk has pursued analysis on other active cases, such as Investigations, KYC (Know Your Customer), Data Management, consisting of data combination, normalization, interconnection, and data securitization, even from various sources of disparate or widely distributed data. They have applied "a scalable data analytics platform, Entity Resolution, Customer 360, Machine Learning Infrastructure, Analytics Modernization, Drug Discovery, Social Network Analysis, Root Cause Analysis, Track & Trace, and Customer Intelligence."

Veeam (2025) recommends that the top 6 ransomware trends that must be watched, accordingly, in 2025 include: "Low Enforcement Forces Threat Actors to Adopt, Data Exfiltration Attacks Grow, Ransomware Payments Are Decreasing, Emerging Legal Consequences of Ransom Payments, Collaboration Reinforces Resilience Against Ransomware, and Budgets Rise for Security and Recovery, But More Is Needed."

Table 3: The World GenAI Adoption Status

Percentage of organizations which have adopted GenAI	65%
Percentage of organizations currently in the GenAI pilot stage	45%
Percentage of the current GenAI projects that are being secured	24%

Source: AI & Data; Leading the AI and Digital Revolution, Worldwide Technology https://www.wwt.com/category/ai-and-data/overview

Without any lack of attention to the dynamic effects of AI on business progress, there are yet many emphatic believers of human creativity in analytical as well as analogical approach and dedication of the employees in achievement of better results. Richard L. Gruner (Winter 2026), in his very latest *MIT Sloan Management Review* article, "Unlock Creativity Through Analogical Thinking," recommends his 4 ways of analogical thinking, including "1. Consume knowledge from distant fields," "2. Be playful," "3. Create safe spaces for speculative thinking," and "4. Evaluate your insights." Hence, one simple implication would be summarized in a conscientious avoidance of letting AI be at the helm of your business.

Veeam (2025), through a broad survey of 1300 global organizations, reported very critically significant findings.

Regarding the need for improvement, as reported in Figures 1, it is so critical that 52% of the respondents believed that a significant improvement or complete overhaul was needed; even more as such, only 11% of the respondents believed that little or no improvement was needed.

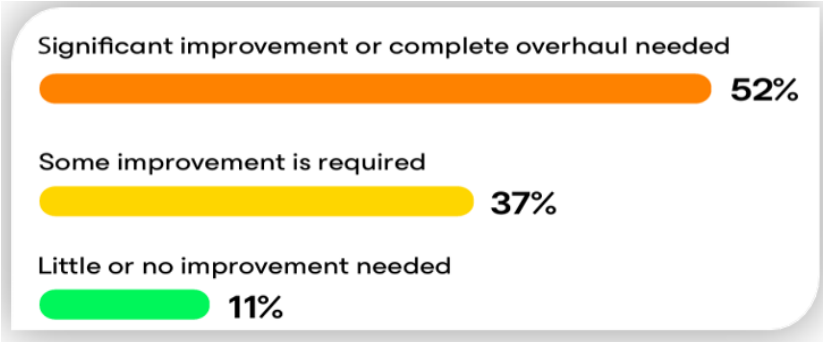


Figure 1: Alignment of IT Operations & Security Teams (1300 global organizations surveyed)

Source: Veeam (2025). 2025 Ransomware Trends and Proactive Strategies

In the same survey, as summarized in Figure 2, regarding cyberfraud and consequential ransom payments by organizations, Veeam (2025) reported that 13% of all respondents paid as much as100% ransom. Meanwhile, 7% paid as much as 76-99%, and 31% of them paid a ransom within the 26% to 50% range. All that would beg for a serious global awareness and a well-calculated responsible formulation - as well as careful implementation - of anti-fraud policies, before this multi-billion-dollar fraud industry, like a fatal harmful apple worm, would find a more destructive way to eat up the remaining undamaged component of the apple, global business and its livelihood. Our model, included in Part II.1 of this research work, as presented in another published work (Hamzaee and Salimi, 2023), would be most appropriate to be re-presented here, as one of the responsive and useful methodologies. Also, in Figure 3, the five mandatory phases of Cybersecurity are recommended to be applied, including direct, protect, identify, recover, and respond, which would have to continue through all available AI, data management, and control operations.

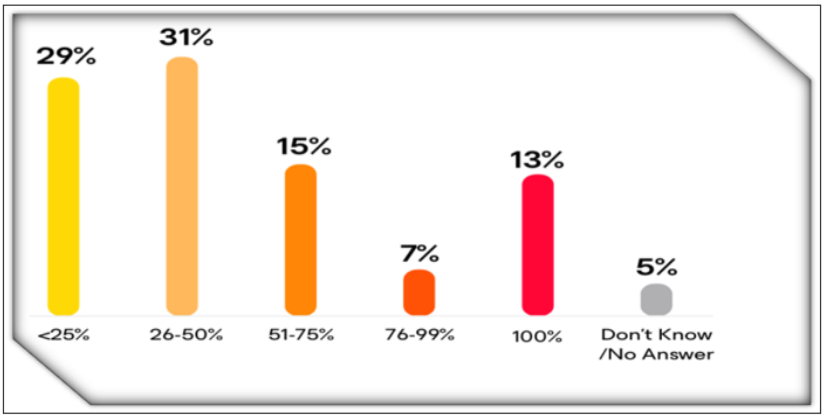


Figure 2: Percentage of Ransom Paid (1300 global organizations surveyed)

Source: Veeam (2025). 2025 Ransomware Trends and Proactive Strategies

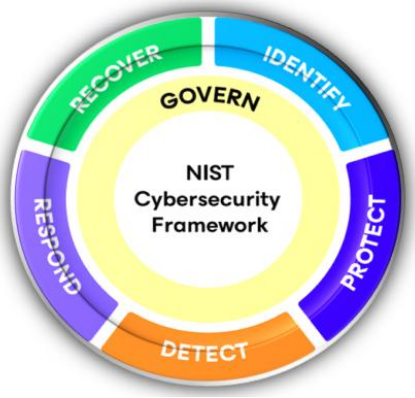


Figure 3: The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0

Source: Veeam. (2025). Building a Cyber-Resilient Data Recovery Strategy

METHODOLOGICAL FRAMEWORK: FRAUD AND ANTI-FRAUD POLICY

In this section, we are offering two theoretical methods, the first of which is facilitating the optimal allocation of resources at an organization to invest in AI and anti-fraud security projects, as depicted Figure 4. The second one is a thorough sophisticated model for an optimal policy formulation in controlling fraud at both national and international industries.

An AI-Blockchain-Massive Data-Based Production Framework

In the following Figure 4, we propose a production possibilities curve (PPC), or the constraint function faced by an organization, and a production isoquant (Q) that represents all possible combinations of the two AI and Anti-fraud (Security) resources to be used that would render the same amount of organization's Q, given all other necessary resources. Obviously, the larger the amounts of any other necessary resources utilized in production of the output, the further the amount of Q would be possible to achieve, all represented, correspondingly by a right-ward shift in the isoquant. However, the main constraint for each organization would be its PPC.

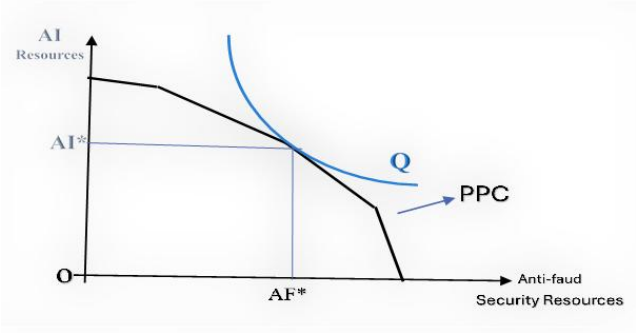


Figure 4: Optimization of Resource Allocation to AI & Anti-fraud Security Projects

Another obvious issue to consider is that, given the nature of the variables involved, i.e., being discrete or continuous (changeable in infinitesimal units), the shape of each of the two curves, Q and PPC, would be either broken (the PPC here), or a continuous function (as the Q Isoquant is assumed). In a practical world of business, both types of variables are adopted to represent some blocks of changes, such as blocks of $1,000, as opposed to infinitesimal fractions of units, i.e., some perfectly divisible sub-fractions of dollar allocations to each of the two resources.

Massive Data-Based and Vector Autoregressive Regression (VAR) Approach

If the time series data on corruption and its various subcomponents, as discussed above, are all collected and recorded, one can generate a VAR model for the inclusion and implementation of artificial intelligence, as summarized below. All the variables are defined in Tables 4 and 5.

Table 4: The Most Common Occupational Fraud Schemes in the United States & Canada

Item	Variables Defined	Fraud Categories	Percent of Cases
1	CORR	Corruption	37%
2	BILL	Billing	24%
3	NCAS	Noncash	18%
4	EXRE	Expense reimbursements	17%
5	PRLL	Payroll	16%
6	CPTM	Check and payment tampering	15%
7	SKMG	Skimming	13%
8	CSHD	Cash on hand	11%
9	CSHL	Cash larceny	10%
10	FSFD	Financial statement fraud	8%
11	RGDS	Register disbursements	4%

(Source: The Authors' Arrangement, Data Coding, and Tabulation, Borrowing from Data Analysis from Dorris 2022)

Table 5: The Most Common Anti-Fraud Controls in the United States & Canada Variable Designation

Item	Variable	Anti-Fraud Control Focus	% of Cases
1	COC	Code of conduct	74
2	EAFS	External audit of financial statements	72
3	ESP	Employee support programs	66
4	IAD	Internal audit department	66
5	MCFS	Management certification of financial statements	65
6	EAIC	Externaaudit of internal controls over financial reporting	63
7	HL	Hotline	63
8	MREV	Management review	63
9	IAC	Independent audit committee	56
10	FTE	Fraud training for employees	55
11	FTME	Fraud training for managers/executives	55
12	AFP	Anti-fraud policy	51
13	PDMA	Proactive data monitoring/analysis	43
14	FFRA	Formal fraud risk assessments	42
15	DFD	Dedicated fraud department, function, or team	41
16	SA	Surprise audits	35
17	JRMV	Job rotation/mandatory vacation	20
18	RFW	Rewards for whistleblowers	14

(Source: The Authors' Arrangement & Tabulation, Using Data from Dorris 2022)

Fraud Index and Fraud Control Index

Define the two indexes of fraud and anti-fraud variables for designing our artificial intelligence model of fraud control, as listed in the following 12 equations:

$$\sum_{1}^{k=11} \alpha_{\mathrm{kt}}.F_{\mathrm{kt}} = \mathrm{FI}_{\mathrm{kt}} \quad (1)$$

where, t= time period, k=1 to 11 types of fraud categories (variables), and

$$\sum_{1}^{\mathrm{l}=18} \beta_{\mathrm{it}}.\mathrm{FC}_{\mathrm{it}} = \mathrm{FCI}_{\mathrm{it}} \quad (2)$$

where, i=1-18 types of fraud-control categories (variables) ,α and *Β* are weights, in percentages, and

- $\mathrm{FI}_{\mathrm{kt}}$ = Fraud Index in Period t for k fraud categories ("variables"),and
- $\mathrm{FCI}_{\mathrm{it}}$ = Fraud-ControlIndex in period t,for i categories "("variables")" of fraud control.

Instead of 11, to make our own model's fraud index, we are adopting the three (as opposed to all the 11) top fraud categories (variables) of CORR, BILL, and NCAS due to their reported top percentages of 37%, 24%, and 18%, respectively, in Table 3. Also, for our anti-fraud control index, we have adopted the top 4 variables of COC (74%), EAFS (72%), ESP (66%), and IAD (66%), listed in Table 4. So, more specifically, equation (1) would be summarized to equation (3) as follows:

$$\mathrm{fI}_t = 0.37\ \mathrm{CORR}_t + 0.24\ \mathrm{BILL}_t + 0.18\ \mathrm{NCAS}_t \quad (3)$$

and equation (2) will melt down to:

$$\mathrm{FCI}_t = 0.74\ \mathrm{COC}_t + 0.72\ \mathrm{EAFS}_t + 0.66\ \mathrm{ESP}_t + 0.66\ \mathrm{IAD}_t \quad (4)$$

In the application of Vector Autoregression (VAR), the number of lags adopted are critically significant in the reliability of the estimation results. The significance of the

number of lags to adopt can be detected within the VAR specifications. Let's define Fraud Index (FI) and Fraud-Control Index (FCI) here, and assume using the relevant data, optimal number of lags would end up being 3. Then the procedure we follow to propose our VAR model, is summarized in the following subsection.

FRAUD CONTROL POLICY VIA VECTOR AUTOREGRESSIVE REPRESENTATION MODEL

Hence, hypothesizing that fraud-control policy (variables) would correspondingly control fraud, incorporating the recent report published by Dorris (2022), there are several procedural regression models to choose from. One way is to just take no prior causality stories or hypotheses. Insert the available data on whatever possible variables that may reveal any relationship between the two groups of fraud variables and the anti-fraud variables. Then, statistically, let the most significant VAR estimation results help in exploring the best causality relationship, through the corresponding variance decomposition, impulse response functions, etc. Among several other choices, we have defined and chosen our Fraud Index in period t (fI_t) to be explained by three lags of itself and the four most heavily adopted (percentage wise) anti-fraud variables, as listed in Table 4.

$$\mathrm{fI}_t = \mathrm{f}\,(\mathrm{COC}_t,\ \mathrm{EAFS}_t,\ \mathrm{ESP}_t,\ \mathrm{IAD}_t) \tag{5}$$

Let's see how many different possible orderings of the above 5 variables we may have in exploring the one with the highest significance:

$$\text{Ordering 1: fI COC EAFS ESP IAD} \tag{6}$$

$$\text{Ordering 2: COC fI EAFS ESP IAD} \tag{7}$$

…… and 118 extra orderings of those 5 variables. Simply because it would be:

$$A_5^5 = \frac{5!}{(5-5)!} = 120 \tag{8}$$

Let us think of AI and blockchain technology, which would broaden the potential capacity of estimation into much more substantiated statistical significance, warranted by so much of observations and massive data registered permanently on the blockchain ledgers. The data already compiled, marked, coded, entitled, transformed, categorized, and would be used through the high-speed software for the best predictions, marketing, resource allocations, election campaigns, targeted communications, political and socio-economic policy decisions, etc. Potentially, as an example, only if a substantiated 5-variable response functions are adopted, there would be 120 possible autoregressive functions (5 variables' permutations, 5 by 5 variables) for the maximal number of options to consider.

$$\mathrm{fI}_t = \mathrm{f}\,(\mathrm{fI}_{t-1}, \mathrm{fI}_{t-2}, \mathrm{fI}_{t-3}, \mathrm{FCI}_{t-1}, \mathrm{FCI}_{t-2}, \mathrm{FCI}_{t-3}) \tag{9}$$

which is the VAR reduced form " " of our two fraudand anti-fraudequations" ("indexes") Assuming that:

$$\mathrm{fI}_t = f(FCI_{t-1}FCI_{t-2},\ FCI_{t-3}), in our VAR format,$$

$$\mathrm{fI}_t = \mathrm{f}\,(\mathrm{fI}_{t-1}, \mathrm{fI}_{t-2}, \mathrm{fI}_{t-3}, \mathrm{COC}_{t-1}, \mathrm{COC}_{t-2}, \mathrm{COC}_{t-3}, \mathrm{EAFS}_{t-1}, \mathrm{EAFS}_{t-2},$$

$$\mathrm{EAFS}_{t-3}, \mathrm{ESP}_{t-1}, \mathrm{ESP}_{t-2}, \mathrm{ESP}_{t-3}, \mathrm{IAD}_{t-1}, \mathrm{IAD}_{t-2}, \mathrm{IAD}_{t-3}) \tag{10}$$

More specifically, equation (11) can be re-expressed as:

$$fI_t = a_0 + a_1\, fI_{t-1} + a_2\, fI_{t-2} + a_3\, fI_{t-3} + a_4\, COC_{t-1} + a_5\, COC_{t-2} + a_6\, COC_{t-3} + a_7\, EAFS_{t-1} + a_8\, EAFS_{t-2} + a_9\, EAFS_{t-3} + a_{10}\, ESP_{t-1} + a_{11}\, ESP_{t-2} + a_{12}\, ESP_{t-3} + a_{13}\, IAD_{t-1} + a_{14}\, IAD_{t-2} + a_{15}\, IAD_{t-3} + e_{fI_t} \quad (11)$$

Through VAR estimation, and the corresponding variance decomposition analysis, we can estimate the impact of any one standard deviation change (shock) in each of the right-hand side variables on the targeted (left hand side) variable, our Fraud Index, FI_t, at any period, t.

To verify how stable our estimation results would be, Impulse Response Functions (Figure 5) would be so useful: All possible fraud components and variables that may influence any targeted policy variable, such as FI, or each of the separate components of fraud, such as CORR, are inserted into many regression equations of each given variable, regressed on several lagged values of itself as well as those of the other hypothetically-possible relevant variables. There are many possible autoregressive impulse response functions that can be printed and adopted. Figure 16 exhibits only three for U.S. - Canada impulse response functions for FI_t, our own defined fraud index, reflecting the responses of FI to a shock (a one standard-deviation change) in COC, code of conduct established, EAFS, external audit of financial statements, and MCFS, management certification of financial statements, all detected in the adopted world sample organizations by Dorris (2023), as three selected measures of adopted anti-fraud policy.

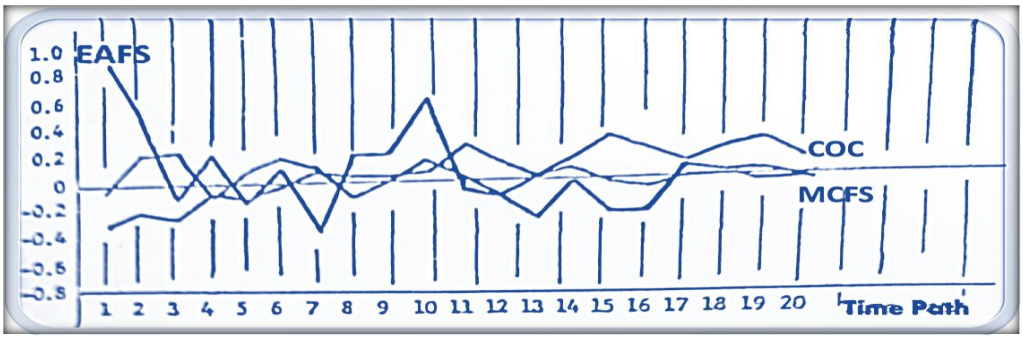


Figure 5: A Hypothetical-Theoretical Example of Impulse Responses of the Integrated USA & Canda's Fraud Index to a One-Standard Deviation Shock in Anti-Fraud Control Variables, EAFS, COC, and MCFS

Source: Hamzaee and Salimi, 2023

The reason we should discuss that potential number of impulse response functions is that the ordering of the variables is sensitive in rendering various statistical significance. There is a general understanding in the literature that earlier appearance of each variable, as contrasted with the ones listed in the later orders, would appear to reveal relatively stronger explanatory power for that variable (Hamzaee 1987, p. 87 and Litterman and Weiss, 1984). Moreover, the stability, and hence, reliability of those relationships, as hopefully observed through oscillations that would be either minimal, or diminishing into some tighter and flatter ones, or even most ideally, eventually fading away through time path, would be promising, as is here, to the researchers' hope.

CONCLUSION AND SUMMARY

More than anything, this research work is to bring the three major technological legs of efficiency and potential prosperity, namely massive data management through blessings of blockchain technology, and machine learning that would create more accountable estimations and guidelines through some data-based AI models into an integrative and dynamic processing model. Using VAR techniques in a hypothetical setting, we have shown how best the needed time-series data could help in making dynamic models that could be adjusted through time and further observations and variations.

We have focused our attention and sensitivities on the application of that tripod of efficiency and prosperity in alleviating the growing dissatisfaction and pessimistic sentiments in the U.S. and around the world. Business ethical scandals, tax evasion, various types of fraud, dishonesty, and broadly experienced failures from governments to businesses, religious leaders, many celebrities, political leaders, and then obviously, "normal individuals," would be better controlled through more extensively accumulated data, involving blockchain, and AI, and dynamically functioning models for machine learning.

Physicians, policymakers, and economists do similarly need more information and data to have further and easier access to some much better remedial diagnoses of the sophisticated illnesses, unnecessarily experienced by the massive populations in desperate need of better lives.

APPENDIX: THE SURVEY METHODOLOGY

For any further description of our coded variables, refer to the main source, Dorris, B, (2022), as is entirely expressed in the exact quote:

"Occupational Fraud 2022: A Report to the Nations is based on the results of the ACFE 2021 Global Fraud Survey, an online survey opened to 53,118 Certified Fraud Examiners (CFEs) conducted from July 2021 to September 2021. As part of the survey, respondents were asked to provide a narrative description of the single largest occupational fraud case they had investigated since January 2020. Respondents were then presented with questions regarding the details of the fraud case, including information about the perpetrator, the victim organization, and the methods of fraud employed, as well as fraud trends in general. (Respondents were not asked to identify the perpetrator or the victim.) We received 7,890 total responses to the survey, 2,110 of which were usable for the purposes of the report. The data contained herein is based solely on the information provided in these 2,110 survey responses. Cases submitted were required to meet the following four criteria: 1. The case must have involved occupational fraud (i.e., fraud committed by a person against the organization for which they work). 2. The investigation must have occurred between January 2020 and the time of survey participation. 3. The investigation must have been completed at the time of survey participation. 4. The respondent must have been reasonably sure the perpetrator(s) was (were) identified.

Analysis Methodology PERCENTAGES In calculating the percentages discussed throughout this report, we used the total number of complete and relevant responses for the question(s) being analyzed. Specifically, we excluded any blank responses or instances where the participant indicated that they did not know the answer to a question.

Consequently, the total number of cases included in each analysis varies. In addition, several survey questions allowed participants to select more than one answer. Therefore, the sum of percentages in many figures throughout the report exceeds 100%. The sum of percentages in other figures might not be exactly 100% (i.e., it might be 99% or 101%) due to rounding of individual category data."

ACKNOWLEDGEMENT

The authors acknowledge the most appreciably support of the specialized data provider, Statista, for its generous and voluntarily granted access to our needed components of their useful and extensive data bank. Also, literature and data published by the three institutions: Veeam, DataWalk, Worldwide Technolgy, are surely highly appreciated.

REFERENCES

1. Anderson, E.; Parker, G., and Tan, B. (Fall 2025). "The Hidden Costs of Coding with Generative AI." MIT Sloan Management Review. Fall 2025, PP. 12-14.
2. DataWalk. (2025). Corporate and Financial Reports.
3. DataWalk. (2025). White Papers and Case Studies on Analytics for Fraud Detection, Anti-Money-Laundering, and Investigative Processes.
4. Dorris, B. (2022) Occupational Fraud 2022: A Report to the Nations. Also available at 2022+Report+to+the+Nations.pdf (amazonaws.com)
5. Dyck, A. et el. (2013, February 22,) "How Pervasive Is Corporate Fraud?" Rotman School of Management Working Paper No. 2222608.
6. Embroker. (2023, June 6) "60+ Employee Theft Statistics for 2023." https://www.embroker.com/blog/employee-theft-statistics/
7. Feedzai. (2025). 2025 AI Trends in Fraud and Financial Crime Prevention. U.S.A.
8. Gruner, R. L. (Winter 2026). "Unlock Creativity Through Analogical Thinking." MIT Sloan Management Review.
9. Hamzaee, R. G. and Salimi, M. (2023, September 25) "Applied Artificial Intelligence, Big Data Adoption/Avoidance in Public Relations, a Proposed Applied Optimal Economic Policy Model and Examination." Archives of Business Research, Society for Science and Education, UK, Vol. 11, No. 9. DOI:10.14738/abr.119.15566. pp. 249-258.
10. Hamzaee, R. G. (1987) Fiscal & Monetary Policy: An International Perspective. Copley Publishing Group, Littleton, Massachusetts 01460, U.S.A.
11. Isik, Oyku; Goswami, Ankita. (Winter 2026). "The Three Obstacles Slowing Responsible AI." MIT Sloan Management Review. PP. 70-74. U.S.A.
12. Jun Ma, B., and Saenz, M. (Fall 2025), "AI Can Improve Humans and Robots Work." MIT Sloan Management Review. Fall 2025, PP. 79-83.
13. Litterman, R. B. and Weiss, L. (1984, January) "Money, Interest Rates, and Output: A Reinterpretation of Postwar U.S. Data." Research Development working paper, Federal Reserve Bank of Minneapolis. Minnesota, U.S.A.
14. Manthena, A. (2025). "CFO's AI Survival Guide: Skills You Need Now. Oracle NetSuite.

15. Ramakrishnan, Rama. (Winter 2023) “How to Build Good AI Solutions When Data Is Scarce”. MIT Sloan Management Review.
16. Statista. (2023, May 20) Tax Evasion Statistics. https://balancingeverything.com/tax-evasion-statistics/
17. Veeam. (2025). From Risk to Resilience. 2025 Ransomware Trends & Proactive Strategies: New Data on Rising Threats & Strategies for Cyber Resilience.
18. Veeam. (2025). 2025 Ransomware Trends and Proactive Strategies.
19. Veeam. (2025). Building a Cyber-Resilient Data Recovery Strategy.
20. Worldwide Technology. (December 4, 2025). “Rethinking the Enterprise Architecture: AI Will Change Everything You Know."
21. https://www.wwt.com/wwt-research/rethinking-the-enterprise-architecture-ai-will-change-everything-you-know