Shift-left in your fight against supply chain fraud

Received (in revised form): 22nd April, 2024

Norman Katz

NORMAN KATZ

President, Katzscan, Inc., USA

Norman Katz is President and Owner of Katzscan Inc., a supply chain consultancy founded in 1996 specialising in user and technical documentation, software selection and implementation, data analysis and operations improvement. A US and international speaker (60+ presentations) and writer (50+ print and online articles), Norman is also the author of three published books: *Detecting and Reducing Supply Chain Fraud* (Gower/Routledge, 2012), *Successful Supply Chain Vendor Compliance* (Gower/Routledge, 2016) and *Attack, Parry, Riposte: A Fencer's Guide To Better Business Execution* (Austin Macauley, 2020). Norman is an ambidextrous foil and sabre fencer. This is his second article for the *Journal of Supply Chain Management, Logistics and Procurement*; the first was 'How abusive vendor compliance programmes are affecting retail store success', which appeared in the Winter 2018–19, Vol. 1, No. 3 issue.

Katzscan, Inc., USA
Web: www.katzscan.com; Tel: +1 954-942-4141; E-mail: normank@katzscan.com

Abstract

Supply chain operations rely upon various supply chain software systems, centred around the enterprise resource planning (ERP) system. Traditional and still widely utilised and relied-upon audit techniques have addressed the issue of finding problems — particularly fraud — typically too late after they have happened. Inasmuch as the ERP system is considered the business system of record, it may not be the system of origination for every supply chain transaction, meaning that fraud examination needs to look beyond the ERP system and notably before the ERP general ledger. The closer to a transaction's point of origin the unusual behaviour can be detected, the sooner the outlier issue can be fixed, and ideally averted in the future with the right corrective actions taken then and there. This all helps to prevent the problem — the bad data, the offending transaction, and possibly the incorrect goods — from travelling through the supply chain and manifesting into something worse. Ramifications can include knock-on effects to data analysis, impacts to decisions, passing bad information to supply chain partners, conveying the wrong goods and material effects on financial statements. This paper presents a supply chain perspective that reveals just how much control an enterprise really does have over its supply chain transactions, showcases how reactive fraud discovery methodologies remain firmly in place, and offers a more proactive business model that leverages what most companies already have to improve internal controls and decrease incidences of fraud.

Keywords

artificial intelligence (AI), supply chain, fraud, enterprise resource planning (ERP), electronic data interchange (EDI), barcode, automatic identification, radio frequency identification (RFID)

DOI 10.69554/NECG3066

INTRODUCTION

In the discussion of supply chain fraud detection and reduction and the leap to how artificial intelligence (AI) could be beneficial, it is helpful to discern what type of AI would be most useful for determining the type of illicit behaviour we want to find. There are frauds that

happen within supply chains, such as counterfeit products, asset mismanagement and theft of goods. These frauds deal with physical things (raw materials, components, finished goods) that are conveyed through supply chains, as well as the machinery that makes supply chains move, such as forklifts, pallet jacks, lorries and the machinery that creates things. For example, a mismanaged asset may be one that is not maintained to its required schedule, even though it was reported to be done so, or one used for a purpose for which it was not intended or designed. Frauds that involve computer network penetration, hacking or theft of data deal with the technology that supply chains rely upon. These types of fraud typically get lots of media attention.

In this paper, supply chain fraud is focused on the individual transactions and their flow not just within independent supply chain software applications but across and between core supply chain systems. Inasmuch as mistakes happen and bad data tends to be something that companies are constantly trying to remedy, fraud detection and reduction is about catching the outlier occurrences and determining whether something illegitimate is happening. Fraud may not be found via a single transaction, but rather during the course of analysing multiple transactions and noticing a pattern. But catching — and correcting — bad behaviour as close as possible to the point of the action are the goals of supply chain fraud transaction analysis.

Data analysis via data extract is after-the-fact and has allowed problems to pass through. Business rules can provide a data qualification barrier but are generally insufficient to catch more complicated schemes. We need a more proactive and a more comprehensive assessment of whether something amiss is happening. AI is a likely software toolset to use for this purpose. Whether the AI application is generating content or differentiating between defined states or acceptable parameters is what should be driving the decision as to which AI is more appropriate to use at which stage of analysis.

SUPPLY CHAIN SYSTEMS OVERVIEW

The enterprise resource planning (ERP) system is the primary business system that runs companies small and large. It is, by my own definition, 'the system that accounts for how a company operates'. The ERP system is not just the accounting system; it is, moreover, a supply chain system and needs to be considered and established as such. It is a software system of two interrelated but not necessarily equal parts: accounting and operations. If we remove the accounting functionalities, we can still operate our business, we just cannot account for what is operationally occurring. If we remove the operations functionalities, there would be nothing to account for.

There are two core supply chain systems that are natural extensions (integrations) of the ERP system. The first is electronic data interchange (eg X12-EDI in the US; UN-EDIFACT in Europe), where business transactions such as purchase orders (PO), invoices and ship notices are sent and received via standard file formats. The second is traditional automatic identification barcode labelling and scanning applications such as those found in a warehouse or distribution centre for receiving, picking, packing, shipping, inventory counting, transferring from one facility to another and moving within the facility, and in retail stores for point-of-sale (POS).

Radio-frequency identification (RFID), another form of automatic identification, is taking its place either alongside or instead of the ubiquitous barcode label.

These three key supply chain systems, which date back to the 1970s and 1980s, are still the backbone systems of supply chains today. Together, their transactions comprise the fundamental supply chain interactions between customers, vendors and suppliers. And together, the transactions of these three key systems create the foundational supply chain performance metrics used by many companies to judge their supply chain operations and the effectiveness of their suppliers (of raw materials and components) and vendors (of finished goods).

Supply chain activities do not just happen outside the walls of the enterprise, they also happen within the walls in between departments, from one facility location to another, within and across enterprise software systems.

The inbound supply chain

Figure 1 illustrates an example of an inbound supply chain that could fit many organisations.

In the inbound supply chain, a catalyst event kicks off the supply chain activities — I equate this to a little 'big bang', if you will. The catalyst event is the need to acquire something, eg from a store shelf or a warehouse location. Somewhere, from a POS system or an inventory system, an item's on-hand quantity fell below the item's minimum safety stock level, which triggered the item to show up on a report or to cause a purchase order to automatically generate to the supplier or vendor for the reorder quantity.

The thing to acquire will be shipped in, received and likely go through some quality control check. A rudimentary quality check may just determine that the things received were in fact the things ordered, and the quantities received are acceptable, eg either a match to the PO or within variance tolerances to the purchase

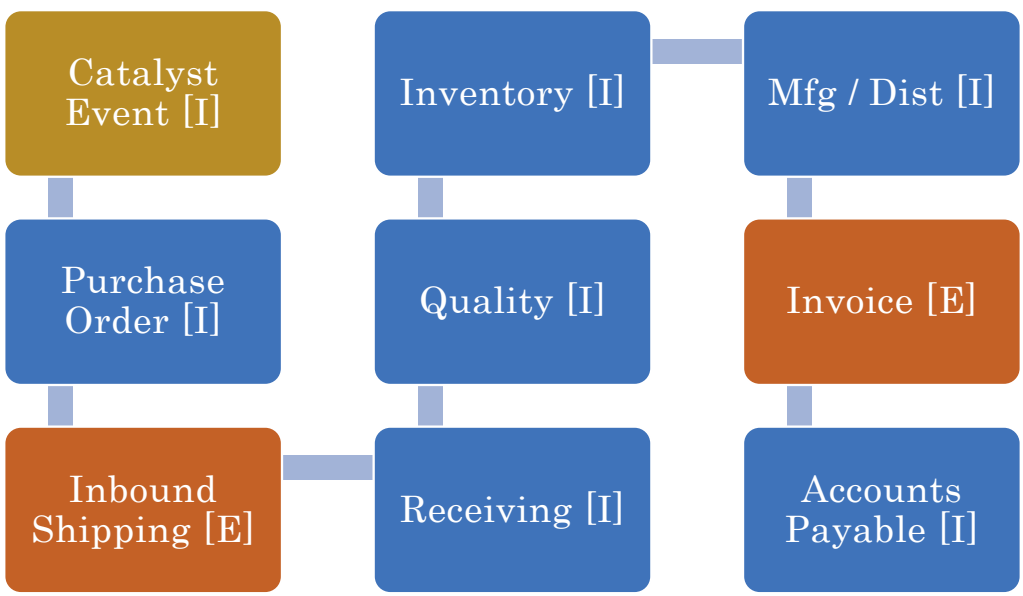

FIGURE 1 Inbound supply chain flow

order line quantity. The received goods will be placed in inventory (the rejected goods go elsewhere) for eventual use in manufacturing or direct distribution. An invoice from the supplier or vendor will generate an accounts payable entry in the customer's (the buying party's) ERP system.

Notice on the inbound supply chain that most of the activities occur internally [I] within the enterprise, rather than externally [E] to the enterprise. Keep this in mind as we take a look at an example of a typical outbound supply chain.

The outbound supply chain

Figure 2 illustrates an example of an outbound supply chain that could fit many organisations.

An external PO (eg as generated in a customer's inbound supply chain) results in and is a sales order to a supplier or vendor in their outbound supply chain. (A sales order can also be created from the action of an online order.) The goods to provide to the customer are picked, packed and outbound shipped (eg scheduling, labelling, documentation, loading). Delivery is probably made by third-party carrier, possibly one contracted by the customer. The supplier or vendor will generate and send an invoice to their customer, which will create an accounts receivable entry within the seller's (supplier or vendor) ERP system. The supplier or vendor may have to pay a sales commission to an internal sales representative or an external marketing firm based on the customer purchase order. And if there are quality issues, the supplier or vendor may have to accept and handle product returns, whether physically in its own facilities, via a third party, or by issuing destroy-in-field instructions.

In the outbound supply chain, notice again that most of the activities occur on the inside [I] of the organisation rather than external [E] to the enterprise. Inasmuch as companies may outsource

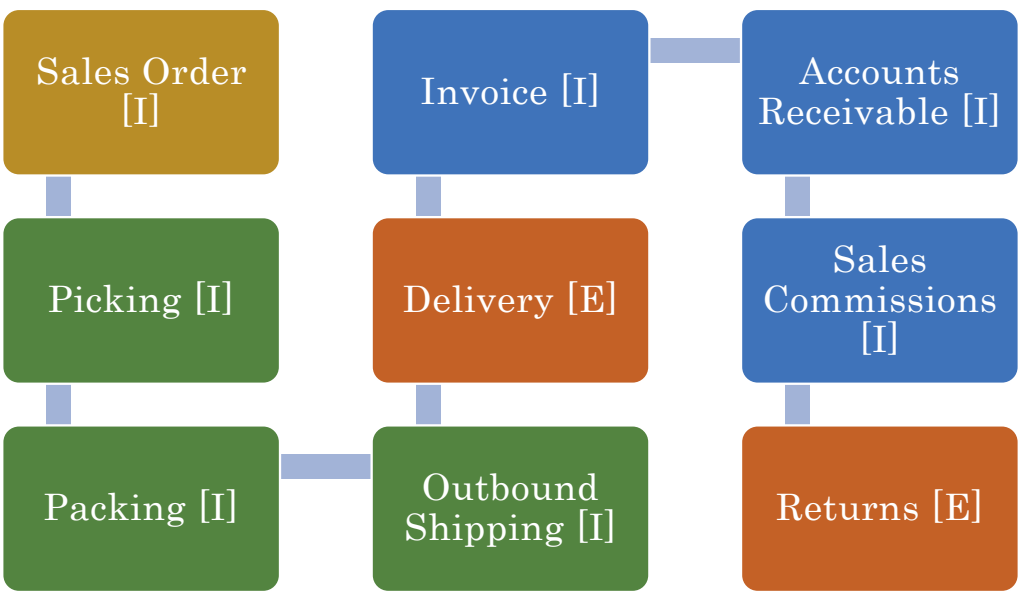

FIGURE 2 Outbound supply chain flow

the activities of contract manufacturing or distribution where picking, packing, and outbound shipping would be services provided, these transactions are still achievable to acquire and analyse, provided they were outlined in the contract.

The inbound and outbound supply chain example flows highlight that most supply chain activities happen within, or at least within the control of, the owning organisation. Therefore, the excuse that supply chain fraud transaction examination cannot occur because the enterprise does not have control of, or cannot gather, the necessary transactions is not really valid. If a company is already examining its supply chain for performance via these systems and transactions, assessing its supply chain for fraud is just as possible.

THE RETURN ON INVESTMENT

Not only is an organisation more in control of its supply chain and the related transactions than it may have previously thought, but the return on investment (ROI) for supply chain fraud analysis is more achievable. Supply chain fraud detection and reduction examination via transaction analysis is really no different from supply chain performance assessment. The same core supply chain systems — ERP, EDI, barcode scanning (automatic identification) — outputting the same transactions that are used for supply chain metrics can be used for fraud analysis. If the Association of Certified Fraud Examiners (ACFE)[1] standard that organisations lose 5 per cent of revenue each year to fraud[2] is used, the justification to analyse transactions already being generated from software systems currently in use becomes a rather easy argument to make.

Both supply chain performance assessment and supply chain fraud analysis examine discrepancies such as:

- Order fulfilment (at the order and line-item levels for item and quantity);
- Quality (first versus other);
- Invoice accuracy (eg total, quantity, credits, adjustments, freight charges);
- Ship-to address verification;
- Shipment total, weight and volume measure based on items;
- Shipment delays;
- Vendor compliance deductions versus chargebacks (financial penalties);
- Mismatched dates;
- Changed addresses;
- Lot/batch identifiers;
- Serial numbers;
- Expiration and warranty dates;
- Transaction response timeliness (eg purchase order and PO acknowledgment);
- Transaction and operation timeliness (eg outgoing shipment and outgoing advance ship notice; shipment physical receipt and advance ship notice receipt).

Suspicious activity is a matter of perspective. From a supply chain vantage point, perfect supplier or vendor performance is the ultimate achievement to be attained. From a fraud examination viewpoint, consistent perfect performance might be an indication that something is just too good to be true all of the time. Layering checks and balances adds confidence that if there is something wrong, it is more than likely a valid concern. Perpetrators of illicit activity can be inside or outside of the organisation. They can be people or software systems, albeit if software systems then they were likely affected first by people, whether innocuously or purposefully.

THE SHIFT-LEFT CHALLENGE

The examination of the ERP general ledger to ascertain whether something is amiss is simply too late in the supply chain activities for detection and reduction of fraud. The issue has not only occurred, but the problem has potentially grown and created other inconsistencies along the way. The organisation is affected, but so too could be supply chain partners as well as data within one or more systems. If the issue becomes material and the organisation is a public entity, there could be credibility issues aside from stock price knock-on effects.

Every two years the ACFE produces its comprehensive global 'Report to the Nations' (RTTN),[3] the latest released in March 2024. This 13th edition pulled together fraud statistics from 1,921 cases from 138 countries and territories across 22 industries and utilised 86 survey questions. (The 2024 RTTN report repeats the 2022 statistic that 5 per cent of revenue is lost to fraud each year in organisations, with the current median loss per case of US$145,000 and the average loss per case of US$1.7m. The 5 per cent statistic — the amount of revenue that organisations lose to fraud each year — seems to have been consistent since I have been a Certified Fraud Examiner [CFE] starting in 2006.) The 2024 RTTN identified the methods by which occupational fraud is detected, shown in Figure 3.

Note: The methods lower than 3 per cent were not shown in the chart for this paper

What the 2024 RTTN data by the ACFE shows is that:

1. Reliance on tips — from inside and outside the organisation — is the most utilised method of catching occupational fraud.
2. Internal and external auditing are effective methods of catching occupational fraud, when used.
3. Automated transaction and data monitoring is not utilised nearly enough despite advances in software capabilities.

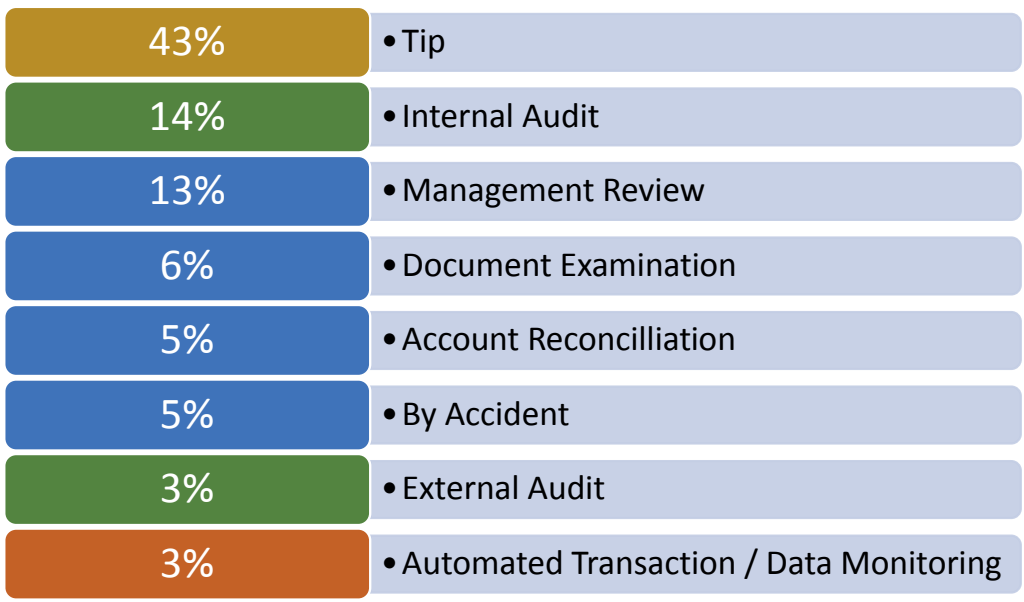

FIGURE 3 ACFE 2024 RTTN: Occupational fraud detection methods

The ACFE in association with the SAS Institute produced the '2024 Anti-Fraud Technology Benchmarking Report',[4] which began in October 2023 and was released in February 2024. The ACFE sent a 22-question survey to over 80,000 members worldwide and used 1,187 of the responses to create the report. While I am not suggesting a direct correlation between the ACFE's RTTN and this technology benchmarking survey, I do believe that we can draw some relationships between the two reports that are relevant and related to this discussion.

If we consider that only 3 per cent of organisations globally use automated transaction/data monitoring as a method for occupational fraud detection based on the ACFE's 2024 RTTN statistics, the ACFE-SAS technology benchmarking survey question 'What data analysis techniques do organisations use to fight fraud?' may shed some detail on the automated/data methodologies used as summarised in Table 1, with my own methodology reference added which will be used in the subsequent table due to space limitations.

What this summary table informs is that AI/ML use is gaining ground relative to other methods. But I would still suggest that this is perhaps within the 3 per cent of overall fraud detection by automated transaction/data monitoring.

The ACFE-SAS report identifies the analytics software used by the survey respondents which I have summarised in Table 2, using the shortened methodology references from the prior table for space considerations.

What this matrix analysis shows is that the top three analytics software programs are Inhouse systems, Microsoft Excel, and Microsoft PowerBI. The In-house systems are noted in the report as being a 'proprietary, in-house platform', so we do not really know anything more about what they are. IDEA and ACL are two commercial off-the-shelf (COTS) software applications known within the audit and fraud examination community.

What the two fraud survey data matrices above tell me is that the primary methods most widely used seem to be more traditional 'data extract and analysis' approaches that are likely reactive to any problems.

Table 3 shows the data matrix of anti-fraud controls used, compiled from separate geographic regional tables in the ACFE 2024 RTTN, and I added the global and regional statistics, ranking by global median.

TABLE 1 ACFE-SAS 2024 report: Data analysis techniques

Methodology	*Author's methodology reference*	*Currently used*	*Expected 1–2 years adoption*	*In use in 2022*	*In use in 2019*
Exception reporting/anomaly detection	ESAD	57%	12%	55%	64%
Automated red flags/business rules	ARFBR	54%	18%	54%	54%
Data visualisation	DV	37%	14%	38%	35%
Predictive analytics/modelling	PAM	28%	22%	27%	30%
Link analysis/social network analysis	LASNA	22%	13%	22$	22%
AI/machine learning (ML)	AIML	18%	32%	17%	13%
Geographic data mapping	GDM	17%	11%	16%	16%
Text mining	TM	14%	15%	16%	18%
Cyrptocurrency tracing/transaction analysis	CYPTA	9%	11%	6%	0%
Emotional tone/sentiment analysis	ETSA	7%	9%	6%	7%

TABLE 2 ACFE-SAS 2024 report: Analytics software used

SOFTWARE USED	*ESAD*	*EFBR*	*DV*	*PAM*	*LASNA*	*AIML*	*GDM*	*TM*	*CYPTA*	*ETSA*	*TOTAL*
ACL	X						X				**2**
Alteryx										X	**1**
ArcGIS								X			**1**
Chainalysis									X		**1**
ChatGPT						X					**1**
CipherTrace									X		**1**
CLEAR					X						**1**
Excel	X	X	X	X	X		X	X		X	**8**
Google								X			**1**
i2 Analytics Notebook					X						**1**
IDEA	X		X								**2**
In-house	X	X	X	X	X	X	X	X	X	X	**10**
PowerBI	X	X	X	X		X	X	X			**7**
Python				X		X					**2**
SAP		X									**1**
SAS		X		X		X				X	**4**
Tableau			X								**1**
TRM									X		**1**
Verafin					X	X					**2**
Total	**5**	**5**	**5**	**5**	**5**	**6**	**4**	**5**	**4**	**4**	**48**

What this compilation of data shows is that *Proactive data monitoring/analysis* ranks overall low globally (15th out of 18 total methodologies) and regionally (between a minimum value of 13 (which translates to 13th out of 18 methodologies) and a maximum value of 16 (which translates to 16th out of 18 methodologies), with both an average and median regional value score of 15 (out of 18) in its use for an anti-fraud control. While this is not to say that other methods do not use any type of software or automation, the point to be made here is that *proactive* data monitoring or analysis is apparently not widely in use, suggesting that other data monitoring or analysis is *reactive*. (I think that this point is also supported by the wide use of Excel and PowerBI.)

This is the shift-left challenge: how can organisations move fraud detection and reduction closer to where the potential fraud is occurring, closer to the originating systems, closer to the originating transactions, and be more preventative and less reactive.

THINK BEYOND FRAUD TO INTERNAL CONTROLS

Fraud occurs across the enterprise in departments that have a direct impact on the internal and external supply chain, its transactions and its stakeholder relationships. As shown in Table 4 from the ACFE 2024 RTTN, fraud does not discriminate where it can perpetrate.

But why should supply chain fraud detection and reduction just be about fraud? Why cannot it also be about reducing waste, eliminating abuse and improving internal controls? It could and

TABLE 3 ACFE 2024 RTTN: Anti-fraud controls used

Anti-fraud control	*AP*	*EE & WCA*	*LA & CA*	*ME & NA*	*SE*	*SSA*	*US & CA*	*GH*	*GL*	*GA*	*GM*	*GR*
Anti-fraud policy	66%	67%	52%	61%	68%	63%	54%	68%	52%	62%	63%	10
Code of conduct	90%	92%	90%	86%	93%	85%	81%	93%	81%	88%	90%	1
Dedicated fraud department, function or team	51%	74%	39%	51%	55%	53%	54%	74%	39%	54%	53%	12
Employee support programs	58%	42%	51%	45%	55%	50%	73%	73%	42%	53%	51%	13
External audit of financial statements	90%	94%	85%	93%	95%	90%	73%	95%	73%	89%	90%	1
External audit of internal controls over financial reporting	72%	79%	67%	75%	89%	74%	67%	89%	67%	75%	74%	7
Formal fraud risk assessments	55%	60%	30%	52%	51%	47%	46%	60%	30%	49%	51%	13
Fraud training for employees	70%	68%	58%	65%	66%	63%	61%	70%	58%	64%	65%	9
Fraud training for managers/executives	66%	62%	57%	61%	64%	60%	61%	66%	57%	62%	61%	11
Hotline	79%	88%	77%	76%	73%	70%	66%	88%	66%	76%	76%	6
Independent audit committee	73%	79%	71%	74%	81%	73%	57%	81%	57%	73%	73%	8
Internal audit department	86%	88%	79%	92%	92%	88%	69%	92%	69%	85%	88%	3
Job rotation/mandatory vacation	25%	18%	21%	33%	36%	23%	19%	36%	18%	25%	23%	17
Management certification of financial statements	80%	76%	76%	80%	89%	82%	69%	89%	69%	79%	80%	4
Management review	78%	80%	68%	80%	85%	67%	66%	85%	66%	75%	78%	5
Proactive data monitoring/analysis	***48%***	***56%***	***30%***	***55%***	***47%***	***39%***	***48%***	***56%***	***30%***	***46%***	***48%***	***15***
Rewards for whistleblowers	15%	8%	5%	28%	29%	13%	11%	29%	5%	16%	13%	18
Surprise audits	43%	55%	32%	62%	49%	44%	34%	62%	32%	46%	44%	16
Regional high	90%	94%	90%	93%	95%	90%	81%					
Regional low	15%	8%	5%	28%	29%	13%	11%					
Regional average	64%	66%	55%	65%	68%	60%	56%					
Regional median	68%	71%	58%	64%	67%	63%	61%					
Regional rank for proactive data monitoring/analysis	15	14	15	13	16	16	14	16	13	15	15	

Note: AP = Asia-Pacific; EE&WCA = Eastern Europe and West/Central Asia; LA&CA = Latin America and Caribbean; ME&NA = Middle East and North Africa; SE = Southern Asia; SSA = Sub-Saharan Africa; US&CA = United States and Canada; GH = Global High; GL = Global Low; GA = Global Average; GM = Global Median; GR = Global Rank (based on the Global Median)

Red highlighting shows the lowest values across the anti-fraud control row for the global regions; green highlighting shows the highest values across the anti-fraud control row for the global regions; yellow highlighting calls out the high values globally and regionally; orange highlighting calls out the low values globally and regionally; light-blue highlighting calls out the average and median values globally and regionally; grey highlighting calls out the ranking values

should be. The great revelation of the Toyota Production System — a precursor to lean manufacturing — is that people on the factory floor could stop production if there was a defect.[5] This is as close to a real-time halt of the offending action as there could possibly be. Recognising that there is a quality issue and preventing it from affecting the current item and manifesting into something worse is the Toyota Production System methodology of 'jidoka', or, as described by Toyota, 'automation with a human touch'.

In combining supply chain performance analysis with supply chain fraud detection and reduction, there is the opportunity to:

- Improve supply chain performance;
- Increase detection likelihood;
- Increase detection thoroughness;
- Increase detection frequency;
- Reduce supply chain errors;

TABLE 4 ACFE 2024 RTTN: Fraud perpetrators by department

DEPARTMENT	*# CASES*	*FRAUD MEDIAN (US$)*	*FRAUD MEAN (US$)*
Operations	221	$100,000	$1,013,000
Sales	199	$75,000	$1,464,000
Accounting	197	$208,000	$1,147,000
Customer service	149	$55,000	$666,000
Executive/upper management	142	$793,000	$4,570,000
Purchasing	107	$143,00	$961,000
Administrative support	94	$88,000	$876,000
Finance	82	$285,000	$2,562,000
Warehousing/inventory	61	$200,000	$1,925,000
Facilities and maintenance	59	$150,000	$423,000
Information technology	51	$156,000	$1,302,000
Manufacturing and production	43	$120,000	$1,974,000
Board of directors	37	$800,000	$4,593,000
Human resources	28	$100,000	$729,000
Marketing/public relations	21	$321,000	$1,415,000

- Decrease fraud probability;
- Decrease fraud impacts;
- Decrease fraud costs.

This can be done without negatively affecting operating costs or having a serious impact on supply chain throughput. Real-time analysis and batch transaction analysis are currently being (should be) performed to catch supply chain errors from a performance perspective. Extra checks at key operations points would be minor compared to the cost of correcting fraud, waste and abuse as it ripples through the supply chain transactionally and physically.

TRANSACTION SOURCE OF TRUTH

In analysing supply chain transactions for fraud, there needs to be an understanding of the source of truth of the transaction: in which software system did the transaction originate? Inasmuch as the ERP system is considered the business system of record, the ERP system is not necessarily the originating system of all supply chain transactions.

PO source of truth

In the example shown in Figure 4, a buying party (the customer) sends a PO to a selling party (a supplier or a vendor).

If we go back to the events of the inbound and outbound supply chains as I represented earlier, a catalyst event will trigger the customer buying party to initiate a purchase order within its ERP system. This ERP purchase order will be transferred to the buying party's EDI system, converted to an EDI PO

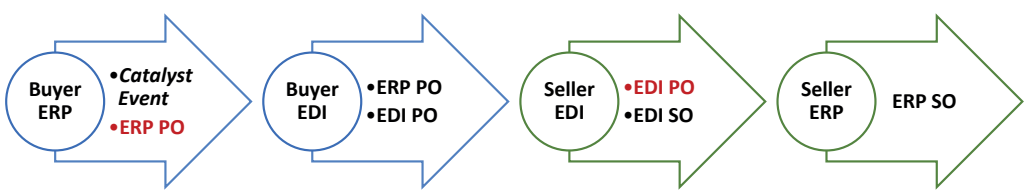

FIGURE 4 Source of truth — PO flow

and transmitted to the seller (supplier or vendor). The seller's EDI system will receive the EDI PO and convert the transaction into a sales order for import into the seller's ERP system.

For the buying party, the PO's source of truth was its own ERP system. For the selling party, the PO's source of truth was its EDI system, not its ERP system.

Invoice source of truth

In the example shown in Figure 5, the seller (a supplier or a vendor) invoices for the PO received from the buying party (the customer) after the related sales order has shipped.

The seller's ERP system generates the invoice from the shipped sales order. This invoice is transferred over from the seller's ERP system to the seller's EDI system, converted to an EDI invoice and then transmitted to the buyer's EDI system. The buyer receives the EDI invoice, transforms it to a format compatible with its ERP system, and imports the EDI invoice into its ERP system.

For the seller (supplier or vendor), the invoice source of truth is its own ERP system. For the buyer (the customer), the invoice source of truth is its EDI system, not its ERP system.

Transaction analysis beyond ERP

The PO and invoice examples were just two of the various that exist across the three core supply chain systems. In the following list, other cross-system transaction examples are highlighted. These transaction matches are typical for supply chain performance but can also be used for fraud detection and reduction. Also note that transaction analysis for fraud requires an examination for the number of transactions in a given timeframe (such as weekly, monthly, quarterly), the monetary amounts on transactions (individual and aggregate) and the quantity amounts on transactions (individual and aggregate).

- PO, PO acknowledgment, advance ship notice.
- PO, PO acknowledgment, receipt.
- Advance ship notice and receipt.
- PO, PO acknowledgment, advance ship notice, receipt.
- Advance ship notice, motor carrier load tender/bill of lading.
- Receipt, quality inspection.
- Invoice, quality inspection.
- Invoice, advance ship notice.

There are other data gaps where fraud can be found too — for example, the difference between customer forecasts, customer sales or consumption data and seller purchasing done to build inventory. A situation where too much inventory exists could be a situation where someone in a seller's purchasing department was illicitly compensated to over-buy. A situation where too little inventory exists could be a situation where someone in a seller's purchasing

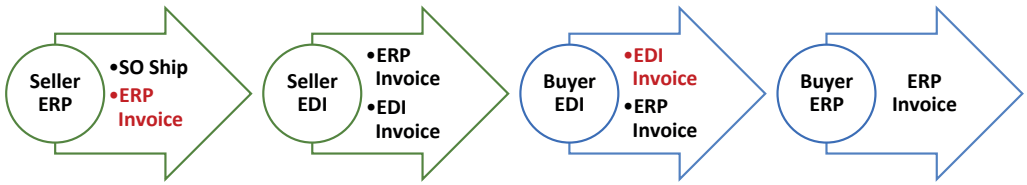

FIGURE 5 Source of truth — invoice flow

department was illicitly compensated to forcibly make an existing supply chain partner provider look incompetent by a competitor hoping to gain a replacement position.

Sales or consumption data from customers should be compared to ERP system shipment information, returns and customer forecasts. This examines for seller company sales commissions to be paid accurately, and relative to any customer returns. Fraud schemes have involved salespeople cajoling customers to buy and overbuy to increase their sales commissions, sometimes with what I will call 'incentives' to the purchasing people. But this only results in the eventual crash when customers have purchased beyond their needs and then try and return the overstock amounts. There can be a material effect on financial statements when this happens.

AN AI SOFTWARE SOLUTION

Using AI to detect and reduce supply chain fraud is not necessarily a one-and-done solution. While this paper is not meant to be definitive on how to use AI, a methodology can be discussed that introduces a framework for an AI solution.

Divide, collaborate, conquer

I believe that the best way to approach the use of AI for fraud detection and reduction (and why not for performance analysis too?) is to first divide the problem by understanding that there are different types of AI that are used for different purposes, eg discriminative and generative.

Discriminative AI is used to differentiate between types of data after there is ML as to where the proverbial line is to be drawn — thus, the name 'discriminative'. This type of AI is useful for determining manufacturing defects where there are deviations from the standard, or where there are exceptions beyond a tolerance level. In using discriminative AI to detect suspected fraud at the point of the transaction's action, transactions that do not match — like those I previously noted — should be called out then and there. It might not mean that there was any fraud (remember, AI is objective, not subjective), but let us expand the hunt for fraud, waste and abuse, and decide that this is about more than fraud but better internal controls. Discriminative AI could be used initially to call out anomalies that should stop processes and allow corrective actions to occur at that point in the supply chain flow, just like in the Toyota Production System. While this will be disruptive initially, all the better to correct the data once at the source than having to correct it multiple times throughout several transactions, and potentially within not just your own company but also with one or more supply chain partners.

Generative AI (GenAI) creates new data from an existing set of data — thus, the name 'generative'. This is the type of AI that creates new text from text prompts and creates new images from text descriptions. After differentiating the 'bad' from the 'good' via discriminative AI, GenAI could be used to gather insights from the 'bad' (and also the 'good') transactions for data patterns that a person would not necessarily find via traditional software tools like Excel, PowerBI, Tableau, etc.

Using both types of AI — discriminative and generative — in a collaborative way could help to conquer the problem of detecting fraud, waste and abuse, and improving internal controls. Individual transaction analysis

and comparison will not always be sufficient to detect all illicit behaviour — batch analysis will still be required — but could be important for stopping some problems from having a ripple effect and manifesting into larger and potentially more expensive issues.

Overcoming the big data barriers

Even if the physical activities of a supply chain are stretched across great distances, the transactions representing those activities are within reach. And as I showed earlier in this paper, these transactions are more internal to the enterprise than they are external, meaning that they are within the enterprise's control. This business model of leveraging existing supply chain systems and transactions to detect fraud dispels the concerns of big data (see Figure 6).

Changing perceptions

In general, the perception of detection is recognised as being a very effective means of reducing fraud. But the perception of detection has got to be real, eg do not install dummy surveillance cameras instead of real, active cameras.

The shift-left of catching discrepancies closer to where they occur is a change in perception too. The recognition that the same supply chain systems outputting the same supply chain transactions can be leveraged for both supply chain performance assessment and fraud analysis is a matter of perception. And once this perception is realised, the ROI for

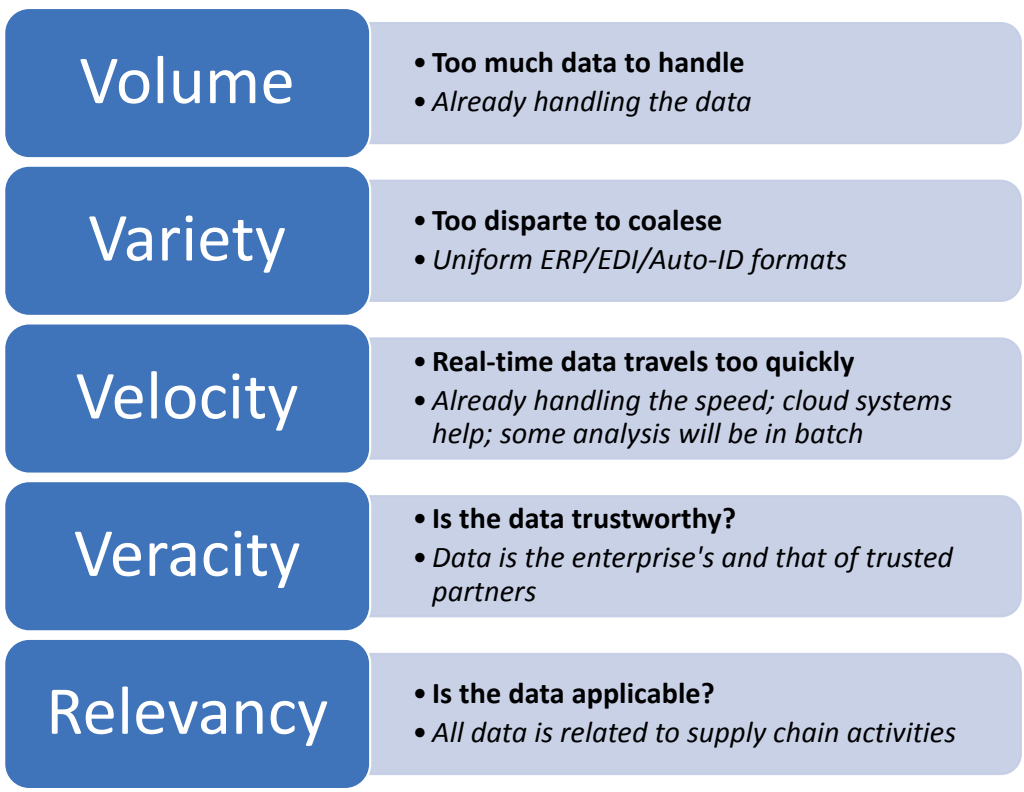

FIGURE 6 Big data barriers broken

improved internal controls and reduced fraud, waste and abuse is readily realised. Catching suspected fraud closer to the operational action does not reduce the necessity of traditional audits, it enhances the overall framework of internal controls and creates a better layering of checks and balances. Risk is reduced and costs are contained.

Balancing risks and rewards

Implementing AI is not without its risks, although it is certainly risky letting fraud run possibly unchecked through a supply chain. The use of AI that I am suggesting here is within the enterprise; it is not one where there is outside-the-organisation interaction. Nonetheless, any such implementation of AI for supply chain performance or fraud detection use should be done with complete user rights-and-roles security and accessibility to only the systems, transactions and data fields necessary.

WRAPPING IT TOGETHER AND WRAPPING IT UP

In its progression, this paper has shown that fraud detection and reduction by means of automation is not a widely used methodology, despite our technological advances on so many fronts. Even where software is used, traditional tools like Microsoft Excel and Microsoft PowerBI are the primary go-to applications. But these are realistically after-the-fact analysis. The illicit action has occurred, and the ripple effect through the supply chain has happened.

Enterprises are mostly reacting to bad behaviour and not proactively addressing it. There needs to be a focus on stopping a problem as close to the occurrence as possible. By letting everyone know that there are effective monitoring tools in place (without necessarily disclosing what those monitoring mechanisms are), bad behaviour tends to go away by itself. Instead of spending time and resources on the hunt for the guilty party, companies should decide to correct issues as soon and as effectively as possible and move on. Remember: everyone is innocent until proven guilty. Whether a mistake or a purposeful manoeuvre, keep your supply chains moving and deal with the root cause on the side without making a snap judgment.

Is AI the right software tool to use for fraud detection and reduction? Inasmuch as the technology is still in its infancy, I do believe that this is the software that is right for this task. I am a firm believer in buying instead of building whenever possible. And we need software that has the ability to 'see' across the enterprise, across different transaction formats, within different enterprise software system databases.

AI is not just one piece of software: it is a suite of software products each being developed by multiple companies, all competing against each other. Discriminative AI is different from GenAI, yet both have their purposes, just like Excel and Word or Excel and PowerBI. Sometimes you will just need one type of software, sometimes you will need a collaboration of more than one type.

By understanding that enterprises can leverage their existing supply chain systems and supply chain transactions for both supply chain performance assessment and fraud detection and reduction, the ROI in bringing in an AI project for this purpose becomes a worthwhile justification. Analysis is only as good as the foundational data. Improving internal controls, getting data accurate, reducing overhead costs, weeding out bad

behaviour … there are positive outcomes from proactive data monitoring.

Companies can start by taking a shift-left and looking at their supply chains differently, taking stock of what systems, transactions and data they have to work with. By changing perceptions on how performance and fraud are viewed as one and the same problem to solve, silos will be broken down and better collaborations will be built between functions such as IT, audit and supply chain operations. The enterprise will benefit overall by leveraging much of what it already has to work with.

In a commoditised world, execution is the new competitive edge. Improving internal controls by focusing on quality is a big part of that. AI is a real possible software solution, but the first realisation is that this is a paradigm shift in how bad behaviour is closely captured, contained and controlled.

REFERENCES

(1) Association of Certified Fraud Examiners (ACFE), available at https://www.acfe.com/ (accessed 22nd April, 2024).
(2) Association of Certified Fraud Examiners (ACFE) (March 2022), 'Organizations Worldwide Lose Trillions of Dollars to Occupational Fraud', available at https://www.acfe.com/about-the-acfe/newsroom-for-media/press-releases/press-release-detail?s=2022-RTTN-launch (accessed 22nd April, 2024).
(3) Association of Certified Fraud Examiners (March 2024), 'Occupational Fraud 2024: A Report to the Nations', available at https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf (accessed 22nd April, 2024).
(4) Association of Certified Fraud Examiners (ACFE)-SAS Institute (2024), '2024 Anti-Fraud Technology Benchmarking Report', available at https://www.acfe.com/-/media/files/acfe/pdfs/sas_benchmarkingreport_2024.pdf (accessed 22nd April, 2024).
(5) Toyota-Europe (2024), 'Toyota Production System', available at https://www.toyota-europe.com/about-us/toyota-vision-and-philosophy/toyota-production-system (accessed 22nd April, 2024).