## 1. PURPOSE

With an estimated 5% of revenue lost by organizations to fraud each year[1], the main purpose of a Fraud Operations ("FraudOps") group is 1) to prevent fraud and bad actors from infiltrating the company and its products, 2) detecting fraud and bad actors should the prevention methodology fail to catch it, and 3) respond to the fraud and bad actors to ensure the activity stops and losses are reduced while also identifying the "how" and "why" of the fraud to prevent it from occurring again.

To accomplish this, FraudOps needs to work seamlessly with multiple other departments as well as create innovative ways to prevent and detect fraud through automation, 3rd party technology implementations, and robust processes. These can be categorized into two main groups- strategic inputs which are forward thinking, scalable, innovative, and solve for long term problems, and operational inputs which are how you make the gears turn and work. Through all these processes, key performance indicators ("KPIs") are used to measure the program's health and longevity as well as appropriate returns on investments ("ROIs").

## 2. STRATEGIC INPUTS

### 3rd Party Technology Implementation

Outside technology implementation is always a positive addition to any fraud program. Although only 37% of companies use this kind of technology, those that do see a 50% reduction in time to identify fraud and overall fraud losses[2]. These types of technology implementations are invaluable as they offer cutting edge systems with tested fraud prevention results, are scalable for future growth, also act as fraud detection, and require little long-term internal resources to maintain.

This technology can aid the company in preventing and detecting some of the key areas of internal risk which include expense fraud, embezzlement, and account takeover and external risk such as ACH/check fraud, credit card fraud, loan fraud, and so much more. Also, with things such as device fingerprinting and similar data sets, 3rd party technology can increasingly aid in detecting organized crime and internal collusion.

### Internal Alerts, Controls, and Continuous Monitoring

Automated and system generated alerts, internal controls, and continuous monitoring are more geared toward fraud detection and are easily adaptable based on the business needs and future growth. As 85% of fraudsters display behavioral red flags[3], alerts should be created that incorporate static rules which identify easy to detect fraud schemes against the company, as well as organic alerts that are more behavioral trends such as velocity rules, % increase/decrease, and outlier detection. Coupling both static and organic alerts ensure a robust fraud detection framework that is specific to how the business operates rather than a one-size-fits-all system.

Alerts and internal fraud controls, such as hold and transaction waiting periods, should incorporate machine learning and artificial intelligence abilities to capture more unique red flags that otherwise may go unnoticed. Knowing that both fraud prevention and automated detection can not identify all areas of risk, continuous manual monitoring is the 3rd key component in which internal departments will frequently review large data sets to detect outliers and red flags that could indicate collusion, new fraud schemes, and the like.

### Feedback Loops

Feedback loops are one of the most vital pieces of a fraud program. Ensuring that key stakeholders are aware of the fraud that is occurring and what FraudOps recommends to stop reoccurrence is key to a feedback loops' success. Data Science is able to take findings and identify trends and gaps which are fed back into the technology to make it smarter. Product and Engineering are able to make updates to internal systems and the actual product to close the gaps and feed the information back into the technology, again making it smarter. Finally, Legal and Compliance can update policies and

[1] ACFE 2022 Report to the Nations
[2] ACFE 2018 Report to the Nations
[3] ACFE 2022 Report to the Nations

procedures to make the process smoother and provide more accountability for bad actors, thus making the product and experience better, and making the technology smarter. The entire process is a circle of communication- feedback loop.

## 3. OPERATIONAL INPUTS

### FraudOps

FraudOps is tasked with identifying areas of risk and providing solutions and recommendations to lower said risk. They will be involved in all fraud processes, including the creating and refining of criteria used to prevent and detect fraud (tech and internal controls). When any potential fraud is identified, FraudOps will conduct a full investigation into the situation and provide findings on who committed the fraud, how it happened, why it was not prevented, and what will be done to ensure the gap is removed thus eliminating, or significantly reducing, the ability for a reoccurrence.

### Human Resources/People Team/Customer Service

HR will be the voice of the employee as well as additional front-line defense in fraud detection with Customer Service being the voice of the customer and, like HR, a front-line defense. They will identify areas of opportunity to improve the employee and customer experience without adversely affecting fraud operations; reducing friction where it isn't needed. They will also help test improvements FraudOps suggests to combat fraud and ensure compatibility and business operational impacts. Also, with continuing fraud awareness training, they will identify weaknesses or possible employee and customer bad behavior through their everyday interactions and refer these concerns to FraudOps for further investigation.

### Engineering

Technology and controls are at the heart of FraudOps' prevention and detection methods and, thus, Engineering is key in making sure those controls work effectively and efficiently. They will reconfigure as needs arise and as FraudOps identifies new fraud trends so internal and external tools can catch and prevent going forward. They will also effectively communicate best practices and opportunities for simplification based on industry standards and make recommendations on possible updates or new technology that could be of benefit to the organization's fraud programs. Lastly, they will continue to iterate on machine learning ("ML") and artificial intelligence ("AI") advancements that can, and are, being used for fraud prevention and detection.

### Data Science

Data Science will continuously review large data sets to identify anomalies and red flags as part of continuous monitoring operations. They will identify fraud trends and possible gaps and forward on to FraudOps for a deep dive. As with Engineering, they will continuously work on ML/AI initiatives and make the technology smarter.

### Legal Support/Compliance

An outside-in view over the entire process is key to ensuring a healthy program, and Legal Support/Compliance take on this role. They ensure that FraudOps are following their own policies and procedures and are ethical in their investigations, while also continuously reviewing laws, policies and procedures, and terms and conditions for opportunities to update and innovate. They will continuously review the process to identify any gaps and make remediation recommendations while also updating when required. Lastly, they will ensure updates adhere to any relevant laws or regulations and ensure that terms and conditions are solid to allow for fraud prevention, detection, and recovery processes to operate at peak performance. (May even be used for restitution and recovery efforts should the company have an appetite, as well as referring cases for prosecution).

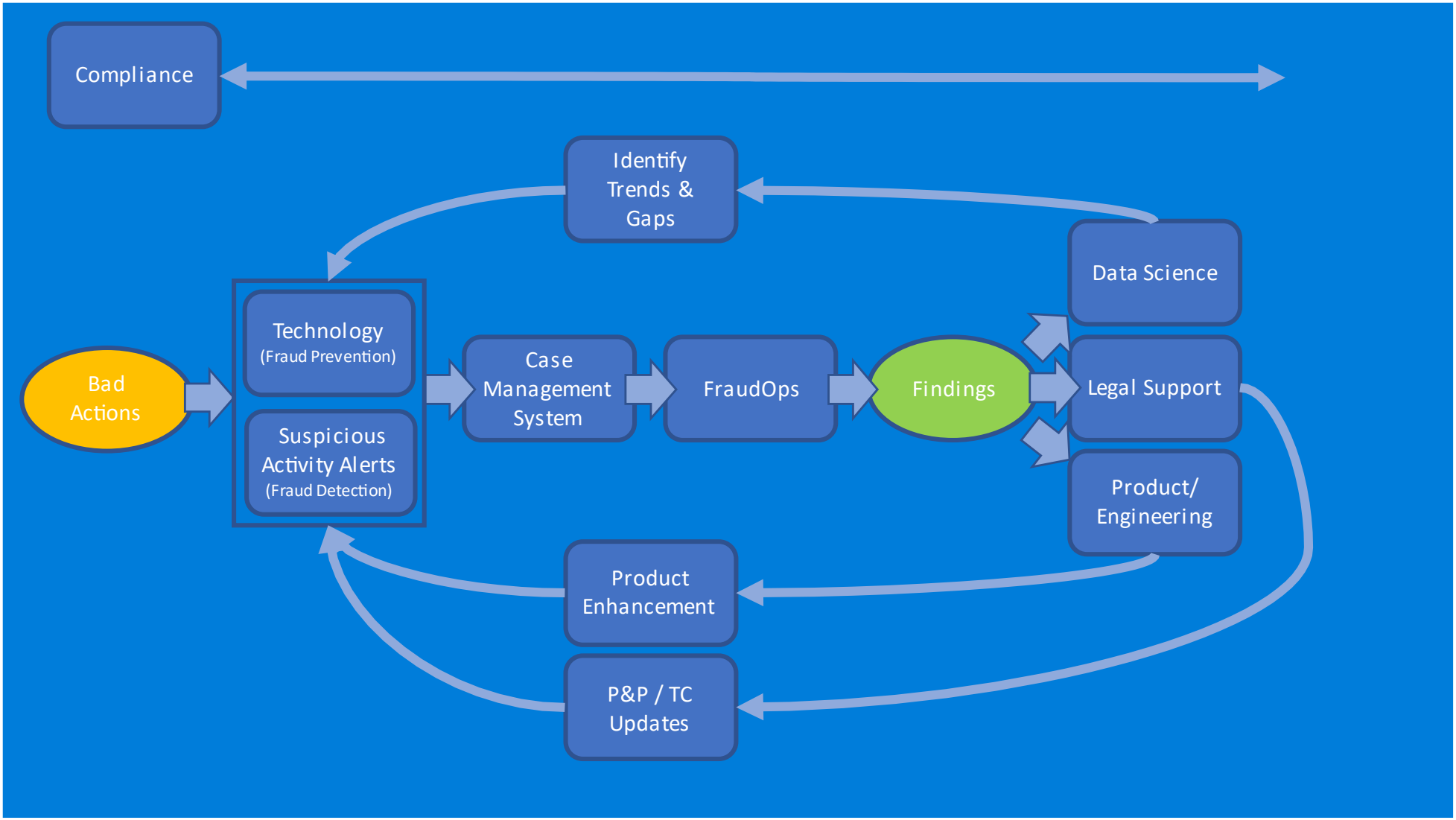
## 4. KEY PERFORMANCE INDICATORS

There are a number of KPIs that are useful to delineate a healthy fraud program from one that may be failing, but there are 5 foundational metrics that should always be included. They are:

1. Rolling twelve-month graph of identified fraud/individuals coupled with fraud losses. These two points will be overlayed with dates showing when certain fraud enhancements were made. This KPI will address the overall trend of company fraud compared to fraud losses and show how enhancements affected them (should indicate a downward slope, otherwise the enhancement may not have worked).
2. Rolling twelve-month graph of incidents grouped by the different fraud schemes. This KPI will allow the company to identify trending fraud schemes and plan future activity (tech implementation or audits) to combat those that appear to be climbing. It will also show the health of fraud program activities by showing how FraudOps is impacting overall fraud trends.
3. Rolling twelve-month graph showing dollar values of fraud losses, fraud losses prevented, and restitution/recovery amounts. This KPI will show the business the ROI of the fraud program.
4. Table indicating fraud program requested enhancements and completed enhancements. This KPI will allow business leaders to see innovative ways FraudOps is tackling its directives and bringing the company forward with less risk. It will also show how FraudOps is engaged with stakeholders and taking partners.
5. Rolling twelve-month graph showing fraud cases investigated, time to completion, and any backlog. This KPI will show the overall health of the department and how service level agreements (SLAs) are being met to combat fraud in a timely manner. It will also help forecast future departmental needs.

## 5. CONCLUSION

As with any fraud program, there are a vast number of moving parts that can affect the success of the department, many metrics to help show the health of a program and forecast needs of the future, and an infinite number of ways to consider how to prevent and detect fraud. The aforementioned inputs, roles, and KPIs are just a few high-level pieces that seem to be foundational to a successful program and with continued communication, feedback loops, controls, and the lot, FraudOps will be on the way to a cutting-edge program where fraudsters pass by knowing they have no chance.


Compliance
Identify Trends & Gaps
Data Science
Technology (Fraud Prevention)
Bad Actions
Case Management System
FraudOps
Findings
Legal Support
Suspicious Activity Alerts (Fraud Detection)
Product/ Engineering
Product Enhancement
P&P / TC Updates