Building
Better Commerce
Fraud & Payments Professionals

MRC Whitepaper

How to Create a Fraud Prevention Unit

MRC Fraud Community
February 2019

Purpose and Evolution

The evolution of any business unit's structure and purpose will be influenced by the overall company priorities, development and growth. Historically, the focus of a fraud unit would often have been preventing or minimizing monetary loss. In this paper, we identify the current focus of a fraud prevention unit of a retail company.

Over the course of time, the operational purpose of a fraud unit expands, as such units migrate into broader functional areas such as chargeback[1] management, fraud management, operational compliance[2] and others. The process of absorbing more functions might be gradual or immediate, often influenced by the internal objectives of the overall company and external factors like industry and geography. In this paper we focus mainly on the fraud perspective. Future papers will cover the broader spectrum.

The role of the Merchant Risk Council (MRC) is to facilitate collaboration between eCommerce payments and risk/ fraud professionals. The MRC received many requests, from its members, for information on how a fraud prevention unit can be established in a company, where no such unit has existed before. The aim of this white paper is to address this and provide best practices.

Dealing with fraud has historically been, and in the foreseeable future is likely to remain, adversarial in nature. As eCommerce sales across the world continue to grow every year, so does the ingenuity of fraudsters looking to steal from merchants selling online; although most fraudsters continue to use the same modus operandi over and again. Having an effective fraud prevention unit is more important than ever. The primary role of the fraud prevention unit is to reduce, as far as possible, losses to the company's bottom line and protect the company's brand and industry reputation. However, there is also a need to ensure the fraud prevention activities of a company are balanced against a positive customer experience and high approval rates.

There is no silver bullet solution to fighting payment fraud. There are multiple companies with unique fraud problems. While this whitepaper is intended to be as comprehensive as possible, it should be noted that as fraud continues to evolve, not all issues can be covered here.

There are many strategies that work which do not all appear here as they may not be openly discussed in an MRC forum. If your organization has an effective approach to fraud prevention and you don't see it here, we would welcome including it in our best practices. Please feel free to email the details to

[1] A Chargeback is normally raised by a card issuer whose customer disputes a purchase transaction (charge) on their payment card. A Chargeback can be raised e.g. when a charge appears on a card that is no longer valid, for a service failure (services not rendered), where the merchant/ acquirer fails to follow payment system rules; or for fraud related queries.
A chargeback effectively means the card issuer returns the value of a sale to the related store/ retailer via their card processor (acquirer). A store can represent a charge if they deem they have the necessary proof to confirm the genuine cardholder authorized the sale in the first instance.

[2] Operational compliance refers to the need for companies/ stores to comply with both the in-house organization operations requirements as well as industry standards (e.g. Payment Card Industry Data Security Standards (PCI DSS), regulation (General Data Protection Regulation (GDPR)), legislation (Payment Services Directive (PSD2)), etc. relating to retail payments.

info@merchantriskcouncil.org with the subject line 'Proposed Fraud Prevention Approach'. The information supplied will be considered in our future updates to this document.

Purpose of the Fraud Prevention Unit

A vast majority of companies within the payments ecosystem believe their business growth and success is reliant on prioritizing marketing and sales. This viewpoint is historically proven, with the exception that no organization can sustain growth and progress without comprehensively identifying and managing fraud risk/exposures. Fraud is an inevitable component of the payments ecosystem and no organization, historically, has avoided exposure to its effects. Previous characteristics are the strongest indicator of future characteristics and it has never been considered a viable option to simply do nothing about controlling fraud and hopefully avoid the consequences.

There are a substantial number of historic examples that demonstrate where companies have been hit by fraud and suffered significant losses and associated reputational impacts. Some of these losses resulted in catastrophic effects on the business, including closure. These losses can have unfortunate and long-lasting effects on a company's ability to remain in business.

Doing nothing is not a plausible or responsible option. A lack of focus on fraud management has such detrimental effects, not only on the company, but on the wider payments ecosystem. Every participating organization in the retail payments industry has a core responsibility to contribute to the elimination of payment fraud and not rely solely on other participants to carry the burden.

The ultimate purpose of the fraud prevention unit is to reduce fraud-related chargebacks, maximize approvals, comply with all legal requirements relating to fraud prevention and to work with the business units to help reduces losses and costs to the company.

Current Environment and Emerging Trends

Fraudsters continue to test payments systems for weaknesses, they re-invent and adapt, and since the fraud scene is continuously evolving, it is safe to say that online fraud is, and will continue to be, a threat.

Customer expectations, when it comes to buying online, are becoming more demanding in terms of ease and convenience. In a very competitive and saturated eCommerce landscape, it is important to find the appropriate balance between fraud, sales and customer satisfaction. This is where a professional fraud prevention team, that understands the fraud landscape and the specific fraud trends that affects each organization, can make a real difference.

Types of Online Fraud

The first step in prevention is knowing the problem and understanding the different types of fraud that are most common today and how they may affect each company.

Note: Visa and Mastercard report fraud under the headings: Lost, Stolen, Account Use, Counterfeit, NRI, Fraudulent Application and Miscellaneous. The core focus here is on Account use/ Card Not Present Fraud.

The list of eCommerce frauds continues to grow every year as new types of fraud emerge. Some emerging fraud types expected to become more prevalent soon are “digital goods fraud”, “return/refund fraud” or “click and collect fraud”, to mention a few. Fraud is described in many different ways and some common types are described below.

- **New Account Fraud** (a.k.a. payment fraud or checkout fraud) is the most common type of online fraud. Fraudsters gain access to stolen card details (Lost/ Stolen Fraud, Account Takeover) and create fake accounts to purchase goods online under the name of the genuine cardholder. Fake accounts can be created by spam botnets or manually by fraudsters. Without any advanced tools and a specialized fraud detection team, it is difficult to identify the real users and differentiate them from criminals using stolen information.
- **Synthetic Profiles** (a.k.a. synthetic identity theft) is like new account fraud, but criminals combine real (usually stolen) and fake information to create a new customer identity, which is used to open fraudulent accounts and make fraudulent purchases or sales online. This type of fraud is on the rise and is usually more difficult to spot, since fraudsters have started aging the profiles for longer amounts of time to make them look more real.
- **Account Takeover (ATO),** where a fraudster gains access to a customer’s account details at the merchant, is an increasing trend. This type of attack can cause real damage, not only in terms of economic losses, but also in terms of credibility and customer satisfaction as the customers negatively affected are your top, loyal and returning customers, which makes it more painful and concerning to merchants. When a criminal gains access to account details, they may be able to steal personal and financial information, place orders with the payment card saved on the account or hide behind the good reputation of an established account to place orders with stolen card details.
- **Mobile fraud** is also on the rise. The increasing use of mobile devices to make purchases and transactions increases the options for fraudsters to find weaknesses and exploit them. Mobile devices can be stolen or cloned and they’re susceptible to hidden malware in apps which gather data, take control of the devices and modify their settings. Since shoppers using mobile devices are more likely to use e-wallets, alternative payment methods like points, credits, or even

cryptocurrencies, it is important to understand and track eCommerce fraud by channel, to identify mobile commerce fraud and create specific fraud detection tools.

- **First Party Fraud** (a.k.a. Friendly Fraud or Cardholder Abuse) occurs when legitimate orders are disputed by the cardholder resulting in purchases being charged back to the retailer and requiring the merchant to refund genuine payments. In some cases, this form of fraud is unintentional, e.g. due to a family member, such as a child, using their parent's payment cards without permission or knowledge, or because they simply don't remember or recognize a transaction. However, in many cases this type of fraud is intentional, e.g. fraudsters placing orders and then claiming they never received the goods.
- **Merchant fraud** is a big problem for Marketplaces. Fraudsters open shops and sell items that are not in their possession, receiving payment for an order they will never fulfill. The business will have to reimburse the buyer for not receipt of merchandise, not only losing money but also affecting their brand and credibility.
- **Transaction laundering** could be considered less a fraud and more a non-compliance with regulation. Fraudsters use fake accounts, that appear to be unrelated, to place seemingly good orders. This way criminals use legitimate websites to move and launder money.

Regulation

Regulation and associated industry standards are implemented globally and at national and regional levels. Compliance with these largely depends on a merchant's geographic location and the territories in which they intend to transact when conducting commerce.

There is high profile, media awareness driven, regulatory standards, e.g. PSD2 and GDPR, that may potentially affect all parties within the payments ecosystem. These need to be understood and adhered to. However, many regulatory standards do not achieve the same level of public discussion and awareness, but inevitably do carry a high level of importance from an operational compliance perspective.

Industry standards can be enforced from a variety of sources including local government, national government, regional monetary collaborations, payment schemes, law enforcement agencies, European Commission, to name a few.

All merchants need to research and comprehend jurisdictional, regulatory implications within their region, and which govern their operational structure. Payments industry regulations and standards are frequently updated and amended to keep pace with growing challenges and risk facing the industry. It remains essential to have a functional structure that facilitates a review of regulatory requirements at an individual and business specific level.

GDPR

The General Data Protection Regulation (GDPR) came into force on May 25, 2018. This regulation provides increased privacy rights for consumers and impacts all cross-border transactions and all organizations that hold data on European Union (EU) citizens. That is, even if this is an EU regulation, it may affect businesses all over the world. If you sell online to EU citizens, you need to comply with the regulation.

GDPR establishes a new and more comprehensive definition of personal data and provides strong guidelines on how companies should handle privacy, store data securely, and respond to security breaches. It applies to data controllers and data processors alike.

Highlights of the regulation include:

- **Information**: Providing consumers with the right to be informed about a data controller processing their information and how to contact them.
- **Access to data and portability:** Consumers can request access to the personal data held on them within an organization and this must be supplied to them in a clear and legible format.
- **Right to be forgotten:** Any customer has the right to have their data completely erased. eCommerce websites should include an opt-out option for the removal or deletion of accounts.
- **Marketing:** potential customers must consent to receiving online correspondence in advance. Additionally, they have the right to prevent automated decision-making, customer profiling and the use of their data to target advertisements.
- **Data management:** organizations should only collect and process personal data for the lawful reasons set out in the GDPR. It cannot be collected and stored because it may be useful.
- **Data breach notifications:** in the event of a data breach, possible impacted customers must be informed within 72 hours.

While the regulation may seem cumbersome to many merchants, the adoption of this new regulation is an opportunity for companies to rethink the way they do business, improve transparency and trust with their customers, and make progress on data security, reducing the threat of breaches.

PSD2 and Strong Customer Authentication

The Payment Services Directive was updated with version 2 (PSD2) and the new version comes into force in September 2019. It will apply to certain transactions where both Payment Service Providers (PSPs) are within the EU. Even though this is a regional directive, it may have a global impact as it will not only affect transactions within the EU but potentially all cross-border transactions.

This initiative was conceived and designed with the intention of creating a single integrated market for payment services by standardizing regulations for the banks and for new PSPs. PSD2 will ensure transparency, fair competition, and break down the entry barriers for new payment services, which will benefit consumers in the long run and help increase competition in the market.

Another focus of this directive is to improve the security and legitimacy of remote payments and online transactions by introducing Strong Customer Authentication (SCA), both for account-based payments (where the consumer logs into an account using a password or PIN to transact online using various payment methods) and card-based payments.

Under the directive, a PSP (note: A PSP can be a card acquirer, transaction processor, solution provider, card issuer, etc. that is, any entity that provides a service within the payments system relating directly to the payment) must introduce a robust authentication process to confirm that a user claiming to be their customer matches the individual who opened the account or enrolled in a service. SCA must include two of three different factors, as follows:

- **Something you know:** something only the consumer knows, such as a password or PIN code.
- **Something you have:** something only the consumer owns, such as a token or a smartphone.
- **Something you are:** something unique that identifies the consumer, e.g. biometric identifiers/ components or behavioral models.

PSD2 creates a new framework and obligations on PSPs however, since SCA often means adding steps (friction) to the consumer journey, certain transactions the PSP processes may be exempt from the need for SCA (such as low value sales, recurring transactions, e.g. a TV subscription, or time critical payments that are deemed low fraud risks) if they are able to implement a secure transaction fraud analysis system that limits fraud.

Transaction Risk Analysis (TRA) is the term for using best efforts to analyze the potential risks in transaction behavior, to identify fraud. PSD2 particularly nudges towards better action and real time detection of fraud through TRA. This was not part of the initial PSD2 draft but was incorporated to address merchant concerns; following a public consultation on the directive.

It is important to understand that this regulation still lacks many details. The most important thing to note here is to keep tracking the changes and adoption of the directive across industries.

Challenges

The introduction of these two important regulations, focused on privacy and eCommerce security, may have an unprecedented impact in the eCommerce fraud landscape. It is likely, however, that fraudsters will focus on ways to overcome, or circumvent the restrictions, look at other methods or shift to other markets. Areas of interest include MOTO (Mail and Phone Orders), exemptions and social engineering.

GDPR and the "right to be forgotten" may create new opportunities for fraudsters. For example, if a merchant allows a user to remove fraudulent data, this creates a gap that could allow fraudsters to repeat their crime as merchants will not have access to some data points they need to update their fraud models or fight chargebacks with compelling evidence. It is important to note that in cases where data needs to be retained for legal or fraud-prevention reasons, there are exemptions.

Under the PSD2, PSPs are obliged to authenticate their customers when issuing payments and managing accounts. The related measures to facilitate this authentication of each consumer can be conceived as friction or barriers to a smooth transaction for the consumer. Purchases or sales may become more complicated which could threaten sale conversions if not managed well.

Fraud Management within the Organization

For any company, there are five primary categories of fraud prevention: strategic, financial, operational, compliance and reputational. Based on the nature of a company and internal organizational structures, these five areas stack differently and often there is no correct order of priority. It is, however, important for the fraud management team to understand what that order is, and how it is evolving. For example, historically, newly formed entities might focus on operational and financial fraud while more mature organizations might be more concerned about compliance and reputational issues. The pecking order might not always be right but, as a responsible fraud team member, knowing these constraints will help you understand how to plan, invest and grow the fraud team.

Importance of Fraud Prevention within an Organization

Different companies place fraud prevention under varying leads and reporting lines. This can tie back to the area of fraud prevention the company deems a priority for the organization. The fraud unit, its internal and external structure, is likely to evolve. It is crucial to track the "fraud prevention appetite" and the importance of fraud management to the organization. This can be identified with a couple of scenarios:

1. **Cost:** Historically, controlling fraud and fraud management has been a cost of doing business. However, a well-functioning fraud unit can be more than just a cost to a business, it can also drive business growth with important and timely input on internal and external developments. The costs to consider include direct costs, e.g. fraud chargebacks and refunds, Operational costs, e.g. people and running systems/ tools, IT costs such as developing capabilities and data. There is the cost of a decline, whether you or the issuer says no to a sale. There are reputational costs, e.g. being an easy target means you get more fraudsters, offering ungainly access means you achieve fewer customers due to high sales friction. Agility costs are incurred when a fraud unit lacks the ability to make changes. A static function always fails.

2. **Scalability:** For a business to scale in a sustainable way, fraud plays a crucial role in ensuring key developments do not increase risk exposure. For many new businesses, there are sudden unforeseen fraud incidents which can hurt growth and similarly for many mature businesses, it is often the gradual, incremental risk exposure that eventually catches up and hurts the trajectory of a company. It becomes necessary for the fraud unit to keep pace and match the scalability requirements of the organization.
3. **Criticality:** The criticality of a fraud management setup is often not appreciated fully until t the time of sizable fraud incidents. It therefore becomes necessary to understand and align the risk appetite of the organization and engage stakeholders in a way to avoid becoming entirely a firefighting unit for the company.
4. **Accountability:** While fraud is most likely to frontload a lot of firefighting when incidents occur, it is necessary for the fraud team to position itself correctly in the accountability setup of an organization.

Fraud Unit Structure and Operational Reporting Links

The “right connections” and “right liaisons” imply the fraud unit is designed in a way that it can communicate well and receive and provide timely updates from across the business. Various companies place fraud prevention under different functions such as legal, finance, customer services and operations, among others. While there are no right answers, and we cannot advocate a best approach, (since historically there has not been much convergence on what structure is most effective), we can advocate setting up fraud officers who can operate across the different organizational functions. Fraud teams tend to deliver when they have strong channels of communication with other arms of the business and have the ear of the leadership whenever there is input to provide. Ensure you operate a risk committee, or equivalent, as a safe place where stakeholders across the company can discuss issues and solutions and help make the hard balance decisions. If you don’t have this set up, there can be friction between the departments.

It is critical for you to encourage coordination and sharing of relevant data between different departments in your company. This practice alone can go a long way towards preventing false declines. For example, if the fraud unit is not informed about sales being offered in certain regions or on certain dates, they won't know to adjust anomaly and velocity thresholds. In this case, not only are these not indicators of fraud, they were probably major sales goals.

Stakeholders to Engage

Within any organization, engaging multiple stakeholders is often routine. There can be fraud originating from a wide range of functions from IT contracts to data acquired and shared for marketing purposes. It therefore becomes crucial for fraud prevention to identify and build relationships with various

stakeholders, both internally as well as with external partners, clients and customers. Such relationships become relevant in the event of a fraud incident or when key fraud-related changes are incorporated.

Framework for Fighting Fraud

Having identified who the key stakeholders and main contributors are, it is important to define a clear framework that manages fraud for the organization in a structured way. To do that, it is important to build a clear framework. In the past it has been typical for a fraud unit to only receive focus from the business when things go bad. Hence, it becomes paramount to define what is in scope (core) for the fraud efforts on an ongoing basis along with provisions for what will be scoped-in when needed (flex). Over time, this classification is expected to evolve. However, if a lot is scoped in (or out) up front, it can make the overall system too rigid (or too lenient) creating problems in the future. The right framework for your company needs can be found by getting three sets of answers – the what, the where and the how of fraud; and bucketing them under your core goals/considerations.

What Types of Fraud to Fight

Due to the rise in volume of digital transactions, coupled with data breaches and other forms of exposure to fraud, there is a myriad of challenges that any fraud unit faces today. This is further exacerbated by toughening data privacy and customer data retention regulations across geographies. All this makes fraud management not only a complex task but also a delicate balance between keeping consumers happy and safe and keeping fraudsters at bay. There are multiple proven ways to design and structure a fraud fighting unit to manage various types of fraud.

Often, financial, operational and strategic frauds dominate general business appetite. It is important for the fraud unit to identify and highlight, exhaustively, how the other two, namely reputational fraud and compliance fraud, can often catch a business off-guard. When identifying financial risk exposure, it is necessary to identify what sort of financial risks need to be prioritized.

The fraud appetite is often a business decision which is why it is important to engage stakeholders and identify which types of fraud are critical to manage for growth and sustainability. MRC resources are useful for putting a business case together to encourage the business decision makers to establish a fraud unit. You can talk about the reasons, the benefits, the risks in not having a fraud unit, etc.

When to Fight

There are two main modes in which a fraud unit can execute: proactive (preferred, but often costly) and reactive which should really be avoided if possible as it is usually too late by the time a fraud unit is established in this way. In the proactive setup, the fraud unit sits alongside other business areas and fraud prevention initiatives help inform business decisions. This is likely to be a more measured and low-risk

approach which might also be slower and often more expensive. For new businesses, it is often hard to estimate how much of an investment in fraud, proactively, is too much versus how much is inadequate. This is why, often, most fraud units operate reactively, at least initially. With a reactive setup, a fraud unit spurs into action as incidents arise and matures defenses as more types of fraud become known. This is true for all companies, regardless of size. It is important to understand that fraud is comprised of knowns and unknowns, making it largely an adversarial challenge, despite best proactive measures.

How to Fight

Irrespective of the type of organizational setup, there are often six key functions a fraud unit always needs to consider: these are prevention, detection, measurement, analytics, investment and communication. The detection and measurement tasks will ideally aim at tracking key business risk numbers to identify when they go off track. The analysis and prevention arms are expected to kick in when that happens, find potential reasons and suggest ways to mitigate them. The communication function, is often implied but is always better to implement as a specific function, aims to manage internal and external stakeholders, clients and partners when a fraud incident happens. Front-ending any of the others to manage communications is usually a recipe for disaster. Someone who identifies a fraud incident (measurement) is likely to size the issue larger than the measures and conversely, someone who analyzes and finds ways to mitigate a fraud in the future is likely to highlight the measures taken.
Investment happens when most of the above functions kick in and allow you to consider whether you outsource your detection tools or build in-house.

While structuring a fraud prevention framework, there are additional important considerations:

- **Build vs. buy:** There are vast numbers of solution providers of fraud fighting components available today. Often some of them are time-tested and some are new and cutting edge. Choosing between them and building something bespoke for your organizational needs should be decided upon based on what the long-term organizational and product goals are, and not simply what is economical in the short-term.
- **In house vs. outsourced:** Similarly, there are multiple aspects of a fraud framework which can be disconnected and potentially outsourced. When doing so, other than various other considerations, an often-ignored aspect is data sharing, storage and management. Your data is most valuable to you, and despite the best legal contracts is important to preserve and secure. Some of the most egregious data breaches and privacy attacks happen on the data hand-off zones between the owner of data and vendors utilizing it.
- **Automation vs. manual:** With the increasing prevalence and mainstreaming of machine learning and other tools to detect and fight fraud, it is becoming a more natural choice to automate fraud fighting. This gives more coverage and easier scalability to any fraud-fighting unit. Here, it is necessary to maintain a balance between how much should execute in auto-pilot mode. Often customers get confused when trying to hurdle across robotic response loops and abandon

products where new users are not treated in an “humane” way. Effectively, the choice can come down to what you sell and what options you have available to you to validate whether the customer is honest or not.

- **Flag vs. enforce:** For many fraud units, it is a difficult call to block/ ban/ remove bad actors vs. keeping tabs on certain behaviors. This is often expected to be aligned with the rest of the business expectations and risk appetite in general. But, risk is usually a careful balance between false positives (identifying a good user as bad) and false negatives (identifying a bad user as a good one). This distribution itself evolves and user behavior often evolves.
- **Contest vs. comply:** When dealing with compliance and chargebacks, there are costs associated with just paying the fees as opposed to contesting them or presenting an argument., etc. These costs vary by market and it is often best to establish a fraud prevention framework which closely aligns to the one which is more economical.
- **Internal and external data:** Most fraud units rely on multiple sources of data, some of which might reside outside of the organization. Acquiring, mastering and storing such data often becomes a critical aspect of fraud fighting. Historically, there have been multiple instances where the data itself has not been managed well and has become fallen to a breach or abuse. Additional monitoring, access controls and regular audits on data, therefore, becomes a core function as the volume of data grows.

Fraud Accountability Framework

This framework is clearly applied to a large well-structured organization and is intended as a suggestion.

Having comprehended. the what, when and how, it is important to establish, maintain and grow the accountability framework.

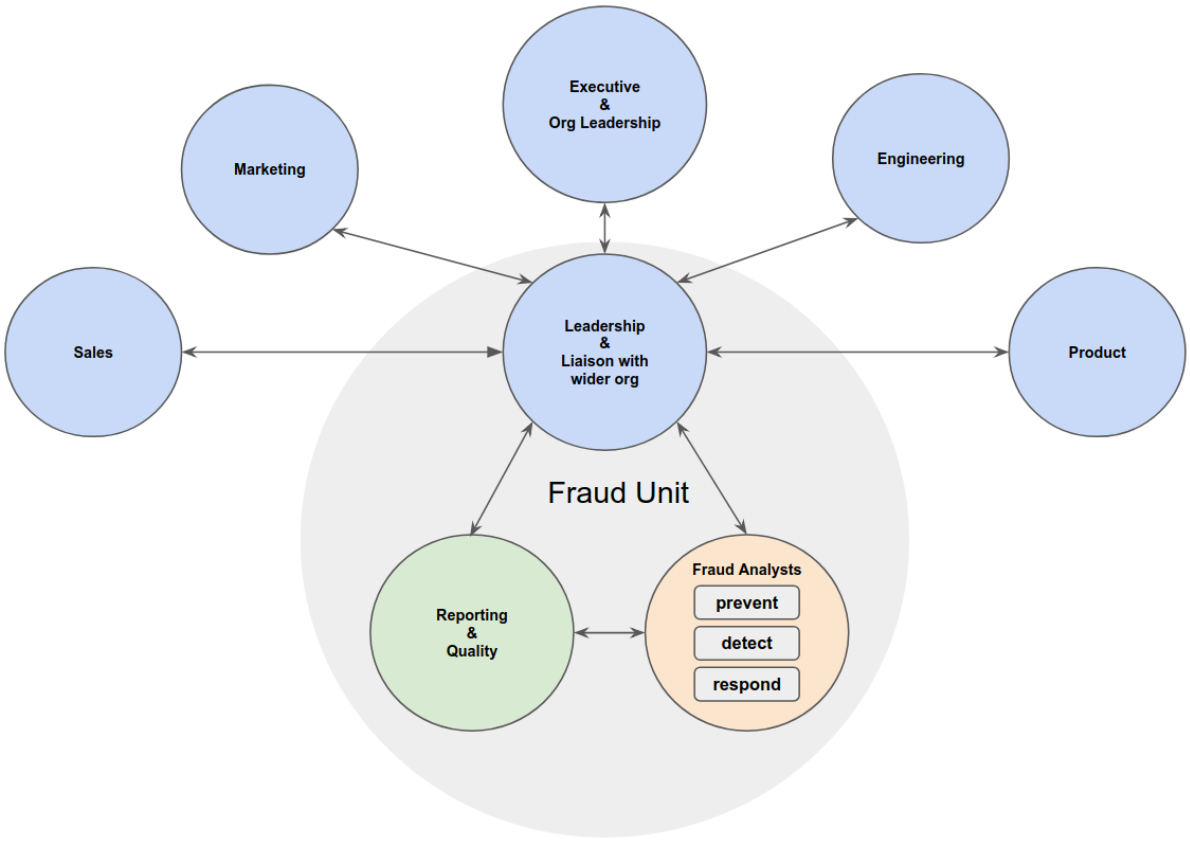
Often, a fraud team's role is seen as that of stopping new user registration and refusing transactions, thereby a system that appears to inhibit growth. A fraud team’s role is to enable “good” revenue growth by mitigating risks and protecting customers. Therefore, the role of a fraud team’s leadership should be to relate to other units in the organization like sales and marketing, product and engineering. This helps build both internal accountability within the team - clarity within the team and external accountability - of the team to the wider organization.

Reporting lines within a fraud team can often range from functional, administrative, geographical or other. We’ll cover them in detail in the “Fraud Team Organization” section that will follow. Whatever the organizational structure a team has, it is, however necessary to create a framework where there is a predefined definition of fraud incidents that are attributable and those that are non-attributable. Attributable fraud incidents are those that are known fraud types which were not handled by the fraud team and similarly non-attributable fraud incidents are those which are completely unknown or new and

only get identified through post-hoc analysis. Therefore, within the team, there needs to be a section which monitors metrics independent of the daily (or regular) fraud management. This team should define and report the fraud numbers and help find the share of attributable and non-attributable fraud.

Within the team, to manage fraud effectively, it is recommended to have separate entities accountable for prevention, detection and incident response. Usually building mitigation for fraud, proactively, can be the responsibility of one team of analysts who can study emerging threats and build countermeasures for them. Similarly, another part of the unit can be dedicated to detecting fraud in ongoing transactions. The third part of the unit can focus on managing users who report fraud incidents and handle follow up until such an incident has been handled.

For the organization, while other teams like sales, marketing and product would often push for pure growth numbers. The fraud management unit's numbers, and by extension, its accountability would lie in reporting the "good" revenue trends. It is also necessary for healthy functioning of the fraud unit as well as for any organization in general to have dependencies and accountability identified more broadly such that teams can rely on each other for information and for better functioning. For example, it would be crucial for marketing to know from the fraud unit that their new campaign is resulting in fake account creation, many of which are getting closed by the fraud unit after a few days of creation. Early information on this can help a new organization save and optimally deploy marketing budget. Similarly, in such an environment, it would be crucial for the fraud unit to know, and plan for, upcoming campaigns, such that they can anticipate and build strong mitigation for keeping bad accounts away from the product.



Overall, it remains the responsibility of the fraud unit's leadership to build a strong internal and external information and accountability framework that supports effective anti-fraud operations as well as promotes healthy growth and effective communication channels

Fraud Team Organization

The organization of a fraud prevention unit will always influence its overall performance. The structure can provide a framework for development and advancement. Many fraud units initially consist of only a few people. If your unit and budget are too small for the headcount, look at the functions performed within the structure. We try to provide our perspective of what an ideal unit could look like based on more established fraud teams.

Fraud Team Unit Structure

First, there should be a department head who is responsible for the strategic and operational roadmaps. This role also usually serves as the interface to the executives of the company with responsibility for budget and reporting. The department head is accountable for ensuring that the department meets its Key Performance Indicators (KPI) and develops its employees as well as its processes for business continuity.

Reporting to the department head are the reporting and quality analysts. Keeping these two functions reporting to the department head keeps them independent of pressure to shade the numbers or favor certain areas over others. A Reporting Analyst should be doing the regular business reporting as well as advanced pattern analysis that forms the basis for new fraud rule authoring. The Quality Analyst should be monitoring orders for process adherence and phone calls for script/process adherence as well as calibrating the quality of customer interactions.

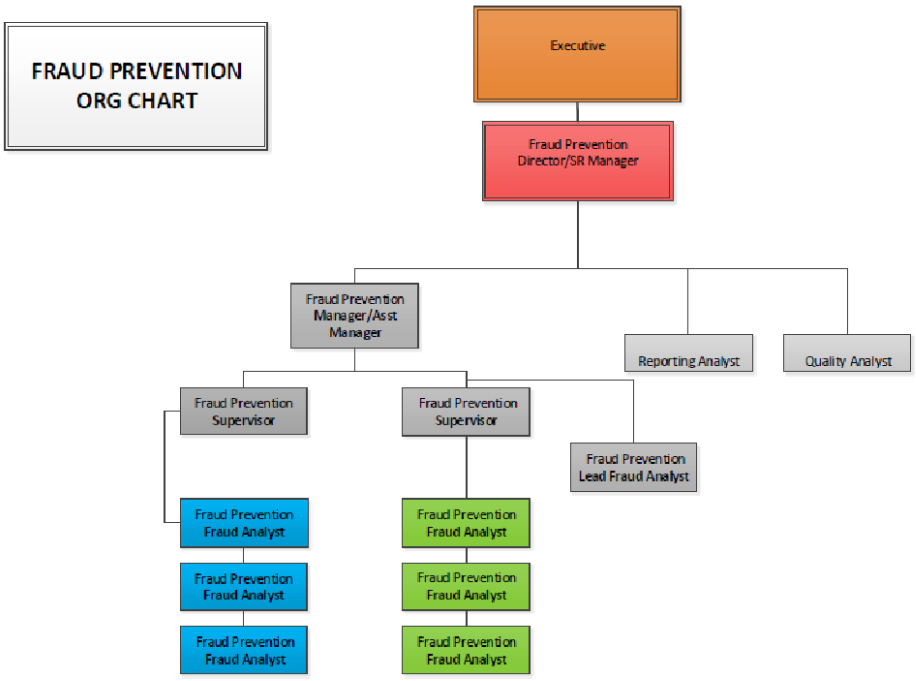
Next is the Operational Manager who focuses on workflow, developing the Supervisors and Lead Analyst, schedules, and ensuring performance appraisals and corrective action (discipline) are conducted fairly and consistently.

The Supervisor balances workloads and priorities, performs performance coaching and corrective action for policy/attendance violations, maintains the morale, and develops the Fraud Analysts for advancement to the Lead Fraud Analyst role.

The Lead Fraud Analyst performs higher level/more difficult transaction reviews, coaches on best practices, and assists the Supervisors with administrative tasks preparing themselves for the Supervisor role.

Fraud Analysts are the backbone of the department performing the manual reviews on transactions the model and rule strategies can’t make a clear decision on.

The important part of the structure of an organization is figuring out the best way to group employees/functions, get the work done and provide opportunities for your employees to develop and grow.



Staffing

Identify the appropriate headcount to meet the organization's fraud goals is often more art than science. It requires a certain element of predictive skills along with aspects of dealing with external forces, including the regulation, internal organizational and industry trends. More importantly, fraud itself and its nature remains challenging and often a hunting game. Here, we outline some well-known ways to predict and staff an effective fraud unit, including good skills to find or hone for strong fraud-fighting teams.

While there is no one-size-fits-all formula for getting ideal team size for a fraud unit. It's a good idea to begin forming a fraud unit by finding team members who map well to the key functions that are important for the team, at first. These internal functions can be mapped to the organization structure with the same person, initially, taking multiple roles, when the team is small, and the scale is more manageable. As the volume and complexity of each function will evolve, more heads would become necessary. Since the quality and reporting function would often provide review and inputs to the regular fraud fighting/analysis function, to start with, it would be recommended to keep the fraud analysis function as distinct as possible from the quality and reporting functions - with separate heads. Later, as a team grows, the team may require more scaling in fraud analysts or on quality specialists or reporting analysts or some combination of them.

In a short span of time, using some of the operational and other KPIs covered in the "Measuring Outcomes" section later, one can identify what areas need more effort and what can be made effective with investment in automation and what areas can be merged with others.

Scaling exactly in proportion to volume of transactions or users often appears easier to do in the beginning, this, however, might create more problems than it can solve. Since a large portion of the unit's role is evolutionary - with adversarial fraud techniques and tightening regulations, the effectiveness and quality of a fraud unit often lies in its agility. It is crucial to build the unit by hiring people who are best suited for the role instead of overstaffing with the wrong kind of individuals.

How to calculate headcount based on expected volume of orders, reviews, and organizational growth projections.

-Determine expected annual volume of orders by count
-Estimate the review rate you believe necessary to meet chargeback target (overestimate a little)
-Multiply your review rate by the annual order volume count to get the annual count of reviews.
-Estimate how many reviews a Fraud Analyst can complete in an hour and multiply by 2080.
-Divide annual reviews by annual reviews completed to get full time equivalents.

The below example uses Using round numbers to illustrate how headcount can be projected. You should substitute your estimates for number of orders, manual review rate, and the number of reviews per hour you believe your staff can complete in the formula below. This is intended to give you a framework and the formula below should be adapted to the needs of your organization.

200,000 annual orders
10% manual review rate
10/hour manual review completion rate

200,000 orders x 10% = 20,000 annual reviews
10/hour x 2080 hours = 20,800 annual reviews completed
20,000 reviews / 20,800 reviews = .96 Full time equivalent or 1 headcount

Key Skills Necessary for a Fraud Analyst
(Note: basic skills will of course vary depending on your analyst needs)

Fraud Analysts are responsible for examining suspected fraud transactions. While hiring for this role, especially for a new fraud unit, there are some key skills and personality traits in its members that would help the unit succeed.

- **Curious/inquisitive:** Many aspects of analyzing fraud and identifying cases involves deep diving and chasing leads. The outcome of many analysis often depends on how persistent an analyst is to find out whether there's fraud or not. This often stems from their curiosity and ability to ask the right questions.

- **Adaptable/flexible:** As outlined earlier, both the nature of fraud as well as the industry and the regulatory landscape continues to evolve. Especially, since the analyst would be far separated from the user and, thereby, fraudsters, the analyst's adaptability remains key to their success.
- **Intuitive/judgement:** Few roles involve making decisions that immediately impact the bottom line of a business as the decisions of a fraud analyst. Having people with the right temperament and decision-making abilities, including the ability to think on their feet, is an important criterion.
- **Team player:** While this goes as a key attribute on almost every job description, a fraud analyst would often need to influence people beyond their own unit, which makes their ability to understand and work in a team, crucial to the success of the organization.
- **Problem solving skills/Analytical:** A substantial portion of an analyst's time would often be spent in working with data and sifting the fraudulent ones from the regular ones. For an analyst to be effective, working well with data and quantitative problem solving would often be essential. This would include, but not be limited to, building and understanding the KPIs as well.
- **Storytelling and creative thinking:** Building the narrative for a fraud scenario and explaining the modus operandi of a fraudster or a fraud signature often requires good articulation skills. This becomes especially relevant when working with or influencing other business units. Most people understand stories better than KPIs and numbers.

People Management Note:

The fraud prevention department has the same people management challenges as the rest of the organization. Although the tasks are different than other departments, the people challenge, and solutions are common. Below are some basic concepts to create and maintain a healthy team dynamic. This team dynamic influences your employees' desire to stay with your organization. Levers that you can pull include pay, employee engagement, incentives, culture, and advancement opportunities.

Pay is always the most difficult to progress, but the best avenues combine tracking and demonstrating that pay is driving your churn and working with your HR department on a market survey of pay for similar positions in your geographic area. When you can show a significant disparity in what similar organizations are paying and that is driving churn which in turn drives down efficiency, accuracy (chargebacks and insults), and training costs you will have the best opportunity to convince your executives that higher pay saves money in the end.

Employee engagement is important because we spend so much of our lives at work. With this investment of time it is important from a satisfaction and performance perspective that you are engaged at work. Ways to drive engagement range from contests, incentives, team builders, stretch assignments, cross training, peer coaching, committees, and management facetime. As you can see, pay and incentives are only some of the tools you have at your disposal to drive employee engagement and satisfaction.

Most of us have occasional team builders to allow our teams to interact off site, or at least off the floor, in a non-work activity. The best ones encourage interaction. For some teams it is competitive events or games and for others it is an ice breaker activity where they reveal personal information about themselves with their coworkers. Going to the movies and sitting in a dark room, not speaking does not advance team dynamics. Combine this with a discussion of the movie's themes, impact, technical wizardry, or relevance to current events and you have a catalyst to improve relationships and communication between the members of your team. While team builders are important, you can combine activity with business tasks, department improvement, and individual development.

Contests that are properly designed drive the behaviors you are looking for in your team. They identify measurable tasks and behaviors that are important for your organization's success. Measuring the results of the contest provides a winner and someone to whom one can aspire. Rewards can be privileges like a temporary schedule change until the next winner is declared, a trophy that travels from desk to desk, a certificate of achievement, an announcement in a department meeting where they are applauded for superior performance, or a gift card, etc. Contests can be designed to reinforce KPI goals or they can be designed to address a current opportunity for team improvement. KPI oriented contests are obvious, but other contests can be very effective in calling attention to other issues where you would like to see improvement. Examples of these include call quality or customer interaction or a most valuable player where the employees nominate the person they feel is most helpful to peers, provides informal leadership and contributes to others' success.

Stretch assignments allow your top performers to vary their daily activities and master new skills. One of the challenges of a manual reviewer is the work is basically the same every day. Unless you are discovering new fraud patterns, today is much the same as yesterday. So, to keep your staff engaged, assign different tasks to them. This can be anything that moves the department forward. It could be administrative tasks, deep dive trend research, coaching a peer whose opportunity area matches their strength area, attending/observing interdepartmental meetings with the manager, updating training documents, you name it. Anything that exposes them to different aspects of running your department to give them more perspective or skill.

Cross training, as discussed above, involves training an individual on new tasks. An easy example is having someone who works domestic reviews learn international, or business, or high dollar or any other segment that your workflow is divided into. This gives your employee a more diverse work flow and improves your department's flexibility in scheduling.

Peer coaching is replicating the best skills across your department. Match people up based on strengths and opportunities. Sometimes the same pair can switch roles as the skill being trained changes. The best way to master something is to teach it. When your team engages in peer coaching both team members benefit. It is also a great way to build team cohesion and comradery.

Committees allow your team members to learn and practice leadership and team working skills. A couple of effective committees would be an event/moral committee and a process improvement committee. One of the ways to reduce workload on the manager and increase employee engagement at the same time is to involve your team in planning events and team builders. Your team members learn about budget, negotiation, team work, planning, follow up, keeping meeting minutes, and leadership. Having your team members do the planning increases their participation as well as their peers. As a manager you get higher participation, greater satisfaction and employee engagement, employee skill and leadership development and, best for you, a little less work. Process improvement committees should be tasked with discussing how to make the process and system utilization better. Most of the best ideas come from the people doing the work. Harness that knowledge and experience with a committee. One of the side benefits is that even the ideas that will not work are an opportunity to educate the committee on system limitations, company culture restraints, budget priorities and other factors they are not normally exposed to. This experience and knowledge pass organically to their team members and helps the organization understand the "why" things can't be done a certain way without it having to come directly from the management team.

Last is management facetime. It is often one of the hardest. Managers are often engaged with other departments, executive leadership meetings, administrative tasks, individual performance coaching, etc. But one of the best gifts you can give your team is your attention. A brief conversation about their family or interests away from work. Discussing their favorite celebrity or sports team can build a relationship that shows you care about more than their performance.

Incentives are an important part of what your employees get from your company. But, if you are only thinking about bonuses and gift cards you are missing out on a variety of non-monetary incentives your team may enjoy, such as flexible schedules, preferred time slot schedules, preferred day of week schedules, reserved parking space, a trophy, posting of KPI or contest results, eligibility to participate in committees or other enrichment tasks/training, praise in a department meeting, recreational facilities, office snacks, coffee, or other recognition. The key is to determine what is broadly appreciated in your department culture. What do they like? Survey them anonymously, talk to them individually, and follow up with satisfaction surveys and questions after you have been running the incentive for a month or two. Chat to your informal leaders and have them help you get answers that some of your team may be too shy to share directly with you. The big key is the incentives are meaningful to THEM. And sure, you can give out gift cards too.

Career development is the process of planning and executing a series of tasks to reach a job goal. This journey is a career. While it is an individual activity and responsibility, organizations can assist their employees in their journey. Organizations can host personality inventories or self-assessments to help employees define their goals. They can also provide leadership training, organizational skills training, Microsoft Word, Excel, PowerPoint, Publisher training, or provide tuition reimbursement for classes that align with the skills needed for the position. Managers can assist with helping employees map out stretch

assignments, training, job-shadowing positions, and identifying a mentor either within or outside the company to provide guidance and support and perspective from outside your department.

Succession planning relies on everything above (retention, incentives, development, and organization chart). Without retention you won't have quality people around long enough to develop them. Without the right incentives, it is more difficult to retain people. If you are not developing your team's individual leadership skills, they will not be prepared to move up into positions of higher responsibility. And without an organization chart that allows for a progression of responsibility employees don't get an opportunity to practice and demonstrate leadership skills necessary to perform in supervisory roles.

Succession planning is critical for the long-term success of the department. If you have not developed a pool of people who are engaged, developing new skills, and ready for the next level you will be crippled if you lose anyone in a leadership role. Whenever you have slack time from operational duties and projects you should be planning how to improve your team's readiness to fulfill the next role and executing milestones on that plan.

Training Resources

Fraud analysts would need skills across multiple areas. Three key areas would be knowledge of tools, understanding of the merchant/payment ecosystem and finally a regular update on emerging fraud trends in the industry.

Knowledge of the tools would usually be organization-specific, including ability to use bespoke tools used within the team for their specific needs. It is a good idea to invest in a knowledge management process which helps maintain know-hows for quick look up and new employee training around tools.

Payments can be an overwhelming space to learn and acquire confidence. A good fraud professional should be able to explain steps performed in a transaction from the user clicking a checkout button to getting an acknowledgement receipt for successful payment. It is good to invest in "nuts and bolts" knowledge of the platform and the overall payments ecosystem for a fraud analyst. Afterall, one needs to know how something works to understand how someone might break in.

The foundations of payments would cover knowledge about the original payment processes involving physical cards (card-present transactions) to more recent forms of checkout including contactless and online payments. Understanding the Payments ecosystem, including details on multiple parties involved in a transaction and how fraud is managed or passed by each entity in a single transaction, is also necessary for members of the fraud unit. Finally, based on the nature of the business and the geography, knowledge and details on authorization and payment authentication is crucial to understand what role the fraud unit can play to mitigate fraud.

Fraud trends and overall industry news are good to keep a track for both benchmarking as well as to be aware of new attacks. Fraud remains an adversarial game and being informed is an effective way to build a strong defense. Newsletters, mailing lists, community memberships and conferences all pay off in some form or the other.

The MRC website (https://www.merchantriskcouncil.org/) contains a wide variety of information and learning tools in its resource center. One popular offering is the Cost of Fraud calculator. This allows businesses to see an example of the potential impact fraudulent transactions can have on their earnings. The MRC operates a mentor program, which pairs fraud and payments industry experts with those wishing to gain from their knowledge. The MRC also offers RapidEdu training courses, providing users with the flexibility to take courses at any time of the day, any day of the year, anywhere in the world.

Measuring Outcomes

When operating a fraud team, it is important to measure outcomes. Although no single metric can define the operations of the team, analyzing a set of KPIs enables the team to maximize their ability to adjust to trends, improve efficiency, and support profitability. Moreover, communicating these KPIs to the broader organization assists with aligning the team with business priorities. For example, some organizations may have a higher fraud tolerance in pursuit of sales, while others may seek to avoid fraud.

This section describes important KPIs and benchmarks that can be used to quickly assess the fraud environment, the performance of the department and individuals. It is not meant to be exhaustive, nor is it meant to address all needs. The section is broken into two: the first describes how to track the broad fraud environment. The measures described herein are concerned with the magnitude of the work to be done. The second describes indicators for operational performance. They cover how the work gets done. It also includes some practical suggestions for tracking and assessing performance.

To fight fraud, managers must understand the fraud faced by the organization. Knowing the amount of fraud, how much was successfully stopped and how much was unsuccessfully prevented are important indicators for operations and the business. The measures included in this section are especially important for setting fraud tolerance and other important actions.

Measuring the Scale of Fraud

Fraud Loss Chargebacks

This measure tracks fraud loss chargebacks over a period. A chargeback is a transaction reversal initiated by an issuing bank, typically on behalf of a cardholder. Cardholders can initiate them for fraud and non-fraud reasons (e.g., service issues), and fraud teams should differentiate based on the reason code descriptions attached to notifications to identify trends and adjust operations accordingly.

Chargebacks are one of the most sensitive metrics owned by a fraud team because they represent potential losses borne by the merchant. Merchants can take the chargeback rate as a baseline from which to improve. However, they should be aware that the chargeback rate can fluctuate due to seasonal trends, the prevalence of fraud rings, tools and processes, and product, among others. Therefore, it should be examined in conjunction with the fraud exposure rate to gain a more complete picture of the challenges facing a fraud team.

Chargeback Representment Win Rate

Notification of a chargeback is not necessarily the end of the journey. Card networks publish guides outlining the information necessary to dispute chargebacks and provide a timeline for the representment process. Disputing spurious charges allows companies to claw back (sometimes considerable) funds. The chargeback representment win rate describes the percentage of chargebacks reversed by the bank and tracks the success of the representment process.

$$Chargeback\ Representment\ Win\ Rate = \frac{Total\ chargeback\ amount\ successfully\ reversed}{Total\ chargeback\ amount\ contested}$$

Fraud Exposure

Fraud exposure is the amount of fraud in a given period. Because it includes both successful (i.e., chargebacks) and unsuccessful (i.e., fraud prevented) fraud, this measure is a baseline from which to judge the fraud threat to a business. Tracking this metric also helps executives understand the scale of the challenge and the dollars at stake. Depending on the focus, it can be expressed either in currency terms or number of transactions.

$$Fraud\ Exposure = Fraud\ Prevented + Fraud\ Loss\ Chargebacks$$

Fraud exposure can be tracked according to many types of data, including by product type, location, and issuing bank, peer analysis, Card Scheme stop lists, declines, chargebacks, refunds, etc.

Fraud Exposure Rate

Higher fraud exposure on its own may not indicate the aggressiveness of fraudsters, if for instance, sales and order volumes might be growing. An alternative measure is to express fraud exposure as a percentage of sales.

Common filters to measure the fraud loss chargebacks are by product type, location, and payment type.

$$Fraud\ Exposure\ Rate = \frac{Fraud\ Exposure}{Total\ Orders}$$

Fraud Loss Chargeback Rate

Like the fraud exposure rate, the fraud loss chargeback rate is simply the percentage of sales that resulted in a fraud loss chargeback. Finding the percentage of transactions that are fraudulent enables teams to understand their chargeback risk as a percent of sales. It offers a method to measure fraud performance over time and across different variables such as product type and location.

$$Fraud\ Loss\ Chargeback\ Rate = \frac{Fraud\ Loss\ Chargebacks}{Total\ Orders}$$

Fraud Loss Rate

Often, customers would approach the merchant to notify fraud issues immediately. Waiting for such transactions to later come through chargebacks can be expensive and may also create a poor user experience. Proactive adjustments are a good way for many businesses to facilitate in such events. These adjusted numbers, however, should also be accounted in the losses as they do not contribute to the good revenue generated for a business. Thus, overall Fraud Loss Rate is represented as Fraud chargeback dollars plus proactive credits for fraud transactions divided by net income.

$$Fraud\ Loss\ Rate = \frac{Fraud\ Losses\ (Fraud\ CB\ +\ Adjustments)}{Net\ Income}$$

Work with your company executives, benchmark with the MRC and peer organizations to set an acceptable fraud loss percentage target for your organization.

For a new fraud unit, chargebacks are a good point to start. However, it is important to note that fraud chargebacks, and chargebacks in general, take some time to mature and come through. Chargebacks are also contestable. So, although chargebacks are an accurate indication of fraud losses, often they may not reveal themselves at the time of a transaction, in fact most don't show up in the same month. As a business matures, it is necessary to find and build leading indicators of fraud. Such indicators can be from customer feedback or other signals.

Operational KPIs

Fraud teams are responsible for much more than identifying and catching fraud. They are important touchpoints on the customer journey, making it essential to accurately track the efficiency and accuracy of operations. Doing so can increase revenue, minimize successful fraud, and maximize customer satisfaction.

Authorization Rate

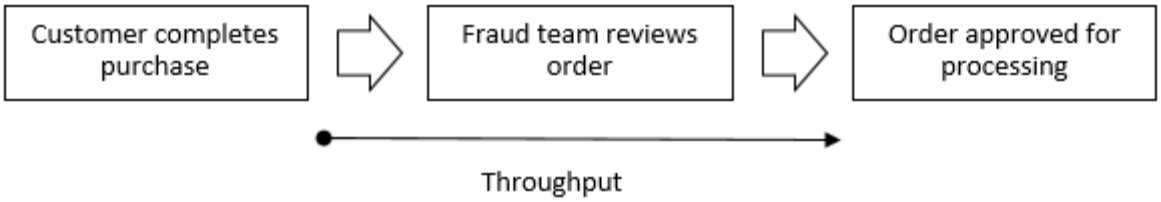
Tracking authorizations falls to the payments, finance, or fraud teams in most organizations, making it an example of the interconnectedness of fraud within an organization. Authorization rates track the number of transactions that were successfully authorized. Although a customer may complete the checkout flow, until the funds are authorized for release, merchants cannot count on the revenue. The authorization rate assesses the performance of the payments system. Although the authorization process is largely outside of the company's purview, a low rate or swings in the rate may indicate an elevated fraud risk or operational issues such as a consistent lack of funds in the customer base.

There are several metrics by which to track authorization rates, including by BIN and by card scheme.

$$Authorization\ Rate = \frac{Successful\ Authorizations}{Total\ Authorizations\ Attempted}$$

Time to Review

This metric describes the time between a transaction submission by the customer and processing. After a customer completes the checkout process and the payment is authorized, it often falls to the fraud team to make the final decision to process the transaction. Doing so efficiently minimizes the impact to the customer. Therefore, tracking this measure enables the team to understand the efficiency of its operations and the resources needed for the review process.



This metric is going to depend on a great many things. Whether your merchandise is physical or digital, your review rate to staffing levels, etc. One way to measure this is to look at the average time between order placement and when the status changes to "eligible to ship" for orders that do not get a manual review. Then measure the average time for manual review orders. Subtract the average time of non-review from review to get the time that the manual review adds to the customer experience.
Determine if that is an acceptable delay and track it over time to reduce it.

$$Review\ Time = Total\ time\ of\ manual\ review\ order - Total\ time\ of\ non-reviewed\ order$$

Manual Review Rate

The manual review rate is defined as the percentage of transactions manually reviewed. Manual reviews are typically slower and more expensive than auto-decisioned ones. Despite their added cost, they can be important to the team's overall performance. To optimize your companies' performance, you will want to find the lowest review rate that keeps chargebacks in check. The fewer you review the lower your expenses will be, the lower your customer insult rate will be and the shorter your shipping delay will be for your good customers.

The purpose of the manual review rate is to track the fraud environment, the efficiency of operations, and other trends.

$$Manual\ Review\ Rate = \frac{Orders\ Held\ for\ Review}{Total\ Orders}$$

Decline Rate

This metric tracks the percentage of transactions that are declined. A high decline rate may suggest false positives or rising fraud risk. Alternatively, a low rate may indicate high levels of fraud. Understanding deviations from a baseline is helpful for organizing the fraud team. Since customer insult is difficult to measure, a good alternative is measuring your reject rate in dollars.

$$Decline\ Rate = \frac{Declined\ Orders}{Total\ Orders} \text{ or } Decline\ Rate\ \$ = \frac{Declined\ Order\ Amount}{Total\ Order\ Amount}$$

False Positive Rate

Fraud teams can expect to misclassify transactions as fraud, and revenue that should accrue to the company is instead lost. False positives are transactions that are declined as fraudulent but are valid. This contrasts to true negatives, which are correctly declined as fraudulent.

The false positive rate is the percent of declines that were incorrectly classified as fraud. Tracking this data point reveals important information for optimizing fraud operations. In some cases, teams, especially new ones, focus on preventing fraud at the cost of not letting through good transactions. In combination with other KPIs, the false positive rate helps teams identify opportunities for improvement.

$$False\ Positive\ Rate = \frac{False\ Positives}{False\ Positives + True\ Negatives}$$

Determining the false decline rate is often a challenge, because there is often uncertainty when reviewing transactions. Several methods exist for estimating false positives:

- **Customer Reorder**: Customers whose transactions are declined may attempt to reorder. If the new one is verified, then it is possible the first transaction was a false positive.
- **Manual Review**: Analysts review declines to identify transactions that should not have been declined. Data science teams can help identify transactions for review.
- **Auto-Acceptance:** Automatically accept a percentage of transactions that would usually be declined and determine how many did not result in chargebacks.

Key Performance Indicators for Fraud Analysts

The following are some Key Performance Indicators that can be used at the individual fraud/ manual review analyst level. This is intended to be an example of how you can measure the performance of your fraud prevention staff objectively and is not an exhaustive list of all the measurable tasks that you may find important for your organization. You may find on some of the metrics below that you would rather measure in dollars rather than a count of orders or vice versa. You may also find that there are more subjective indicators that you wish to include because of their importance to your success or in your corporate culture.

Please use the metrics below as a basis or model to construct the KPIs and weights that you feel drive the success of your business. One important thing to remember is not to create too many KPIs as this does not allow your analysts to focus on what is important. Often three to five metrics is enough to drive the right performance from your team.

Chargebacks Released (Leakage Rate)

To control the financial loss to the company and improve analyst performance, chargebacks released by analysts are monitored and examples coached upon for improvement.

For simplicity, chargeback dollars reported in the performance month regardless of invoice date are counted toward the performance month. This avoids constantly updating performance for previous months. This will even out over the course of twelve months.

$$Chargeback\ Leakage\ Rate = \frac{Total\ Amount\ of\ chargebacks\ from\ released\ orders}{Total\ Amount\ of\ the\ orders\ reviewed}$$

Approval/Rejection Rate

To encourage analysts to release good revenue and good orders with questionable attributes rather than cancel for suspicion of fraud, the percent of orders approved is measured. This metric creates tension with the chargebacks released metric balancing the bias to cancel anything that looks risky.

$$Approval\ Rate = \frac{Count\ of\ orders\ approved\ for\ fulfillment}{Count\ of\ orders\ approved\ or\ canceled}$$

Time to Review

To reduce the shipment delay caused by fraud review and control the payroll cost of the team to the organization, the speed at which an individual analyst works is a good metric to have handy. This may vary by experience of the analyst as well as complexity across reviews.

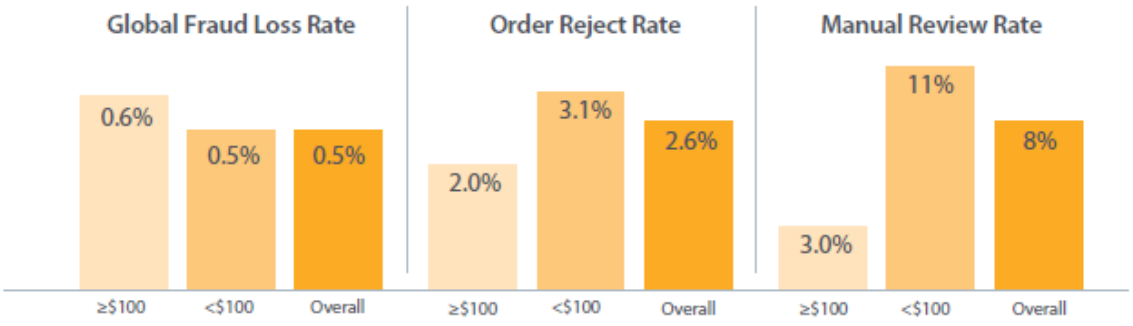
$$Time\ to\ Release = \frac{Minutes\ worked}{Count\ of\ orders\ approved\ or\ canceled}$$

In Appendix 1 we have examples of some of the KPIs above with sample metric achievement bands to show how you would assign scores. Additionally, there is an example of how to assign weights to KPIs and calculations for a weighted KPI score. Weights can change from year to year as your team's emphasis needs to change.

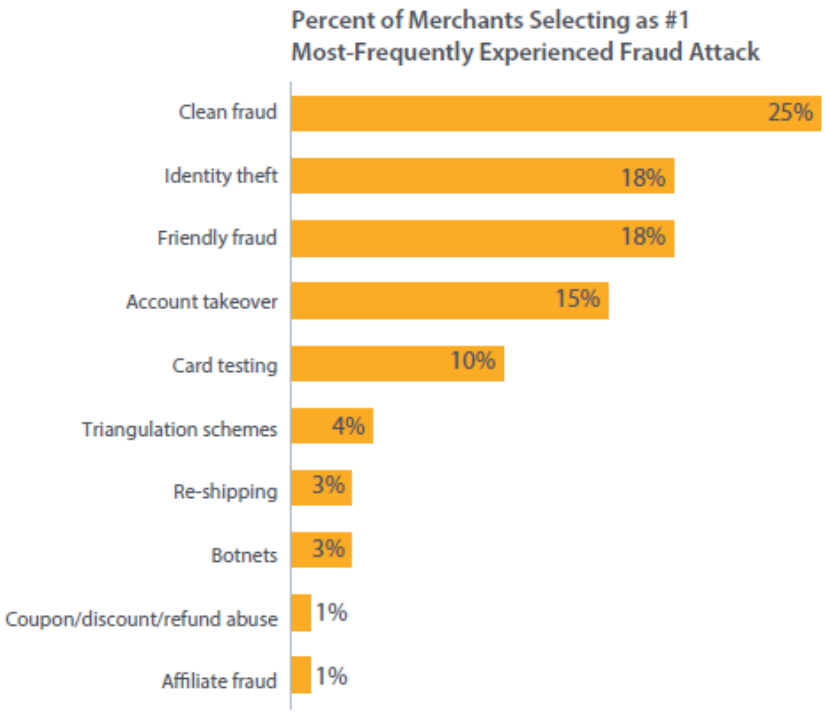
Benchmarking

For any company to measure their performance in fraud prevention with their peers, it is key to examine activities within the company against industry-wide numbers. Following is an excerpt from the MRC Fraud Survey Report 2017 which should be used as an indicator of what a large portion of e-commerce merchants are seeing in fraud [note: this fraud survey report will be updated in 2019 and the results in this white paper updated accordingly at the time].

Fraud by Average Ticket Value

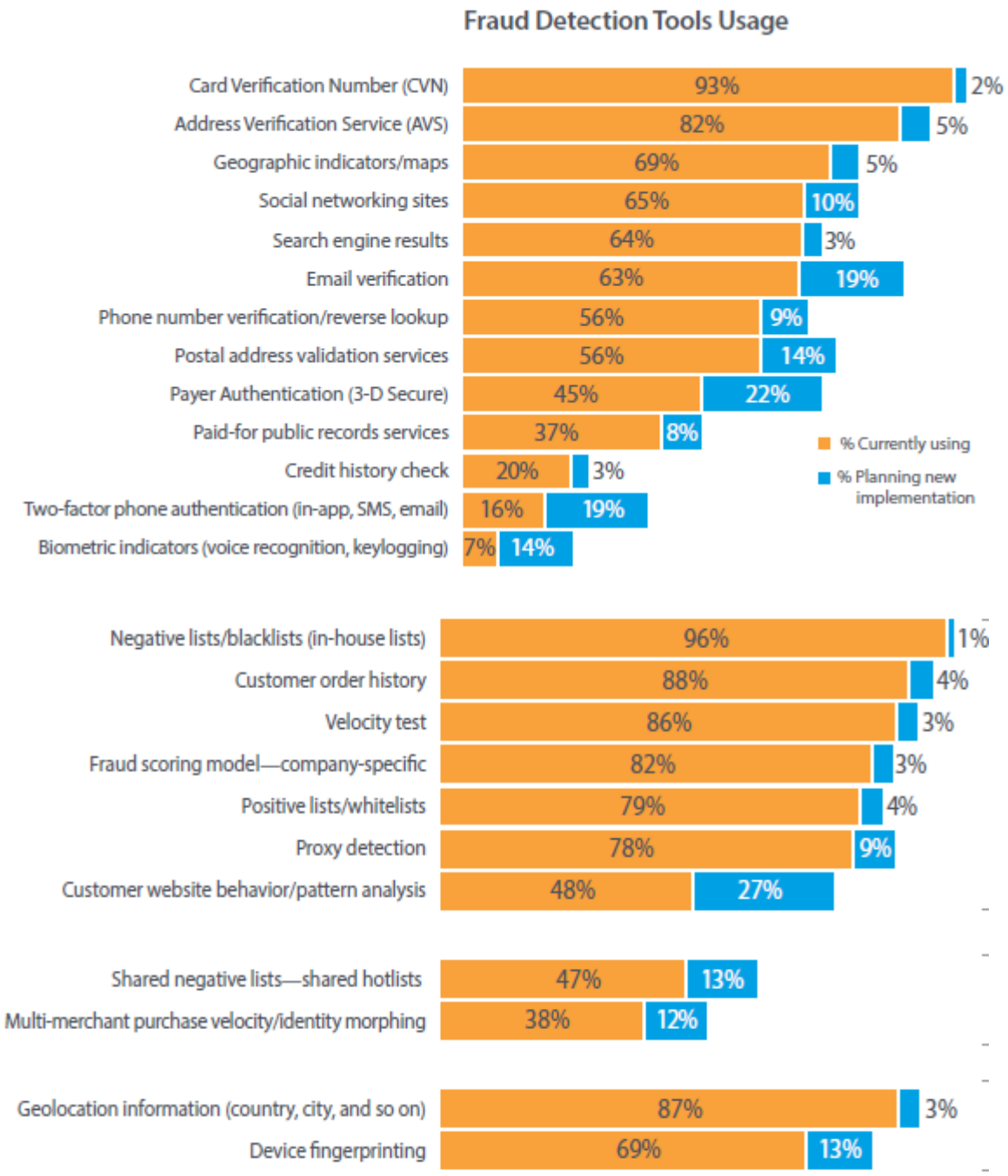


Most Typical Fraud by Type

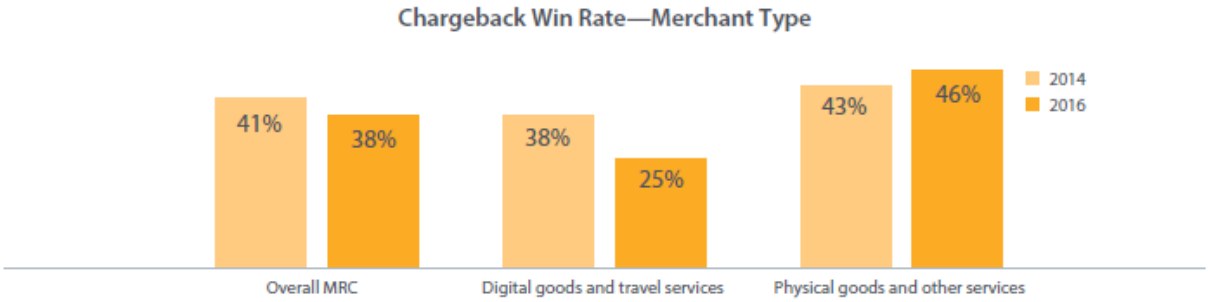


Fraud Management Challenges

Detection – Tools and Techniques



Chargeback Win Rates



Appendix 1

Key Performance Indicators for fraud analysts' calculations

KPI - Chargebacks Released Weight= 35%
Calculation-Fraud CB dollars released/Total dollars released by the analyst

To control the financial loss to the company and improve analyst performance, chargebacks released by analysts are monitored and examples coached upon for improvement.

Score = Metric Achievement
5= ≤ 0.05%
4= 0.06%- 0.14%
3= 0.15%- 0.39%
2= 0.40%- 0.49%
1= ≥ 0.50%

If an analyst got a fraud chargeback on a $700 order and released $10,000 during the month, then $700/$10,000 =.07% of the dollars released by the analyst resulted in a fraud chargeback. They would be scored a 4. (For simplicity chargeback dollars reported in the performance month regardless of invoice date are counted toward the performance month. This avoids constantly updating performance for previous months. This will even out over the course of twelve months.)

KPI - Speed Rate Weight= 20%
Calculation- Number of voided or released transactions/hours worked by the analyst

To reduce the shipment delay caused by fraud review and control the payroll cost of the FP team to the organization, the speed at which the analyst works is measured.

Score = Metric Achievement
5= ≥ 35
4= 30-35
3= 25-29
2= 20-25
1= ≤ 20
If an analyst released or voided 4,160 transactions in a 160-hour month, then 4,160/160 hours = 26 transactions/hr they would be scored a 3

KPI - Pend Rate Weight= 10%
Calculation- Number of pended transactions (held for verification call)/total number transactions resolved by the analyst

To reduce the delay of fraud review and encourage Analyst to release good orders which may have unusual attributes, the rate of orders not immediately released or voided is measured.

Score = Metric Achievement
5= <4%
4= 4% - 6%
3= 6% - 9%
2= 9% - 12%
1= >12%
If an analyst held 10% of the transactions for a customer to call in and verify information they would be scored a 2.

KPI - Approval Rate Weight= 20%
Calculation- Number transactions released/ total number transactions resolved by the analyst

To encourage analyst to release good revenue and good orders with questionable attributes rather than cancel for suspicion of fraud, the percent of orders approved is measured. This metric creates tension with the chargebacks released metric balancing the bias to cancel anything that looks risky.

Score = Metric Achievement
5= >95%
4= 91% - 95%
3= 85% - 90%
2= 75% - 84%
1= < 75%
If an analyst released 87% of the transactions, they reviewed they would be scored a 3.

Extra Duties Weight= 15%

To give analysts the opportunity to get credit for additional work that is intended to develop them for higher level positions or leadership roles in the department an "extra duties" metric can be added to their annual review. In the author's fraud prevention department, all analysts must review their own chargebacks to learn how to prevent releasing future chargebacks. All analysts start with a baseline 2.5 score in extra duties. Each extra duty category performed accurately and on time for the month accrues an additional .5.

- Chargeback Analysis - analysis of own orders released that resulted in a Chargeback
- Law Enforcement - requests for information from law enforcement
- Liaison work with other departments like customer service complaints
- New Hire Training
- Cross Training – best practices or additional work queue

- Voicemails -if your department records them
- Other tasks beyond reviewing transactions for fraud

If the analyst completes the chargeback analysis accurately and on time they would receive an additional .5 on top of the 2.5 starting score for a monthly score of 3. If the analyst is late, their score would be 2.5. If the analyst also participated in cross training during the month an additional .5 would be added for a monthly score of 3.5.

To summarize the weighted score:

	Score	Weight	Weighted Score
Leakage (chargebacks)	4	X .35	1.4
Speed	3	X .25	.75
Pend	2	X .1	.2
Approve	3	X .15	.45
Extra	3.5	X .15	.53
So, the Analyst would score			3.33

An additional measure for a fraud/manual review agent would be customer insult. One way to measure this would be customer complaints divided by transactions canceled. This could be measured in count of orders or sum of dollars. If you track and measure this over time you will find where your team bunches up and then you can create a scale for your metric achievement.

Acknowledgments:

The Merchant Risk Council would like to thank the following companies for their representatives' contribution to this White Paper, each of whom is a member of the MRC Fraud Committee.

Google
Epoch
Etsy
Newegg
Blueport
Riskified
Visa
Sony