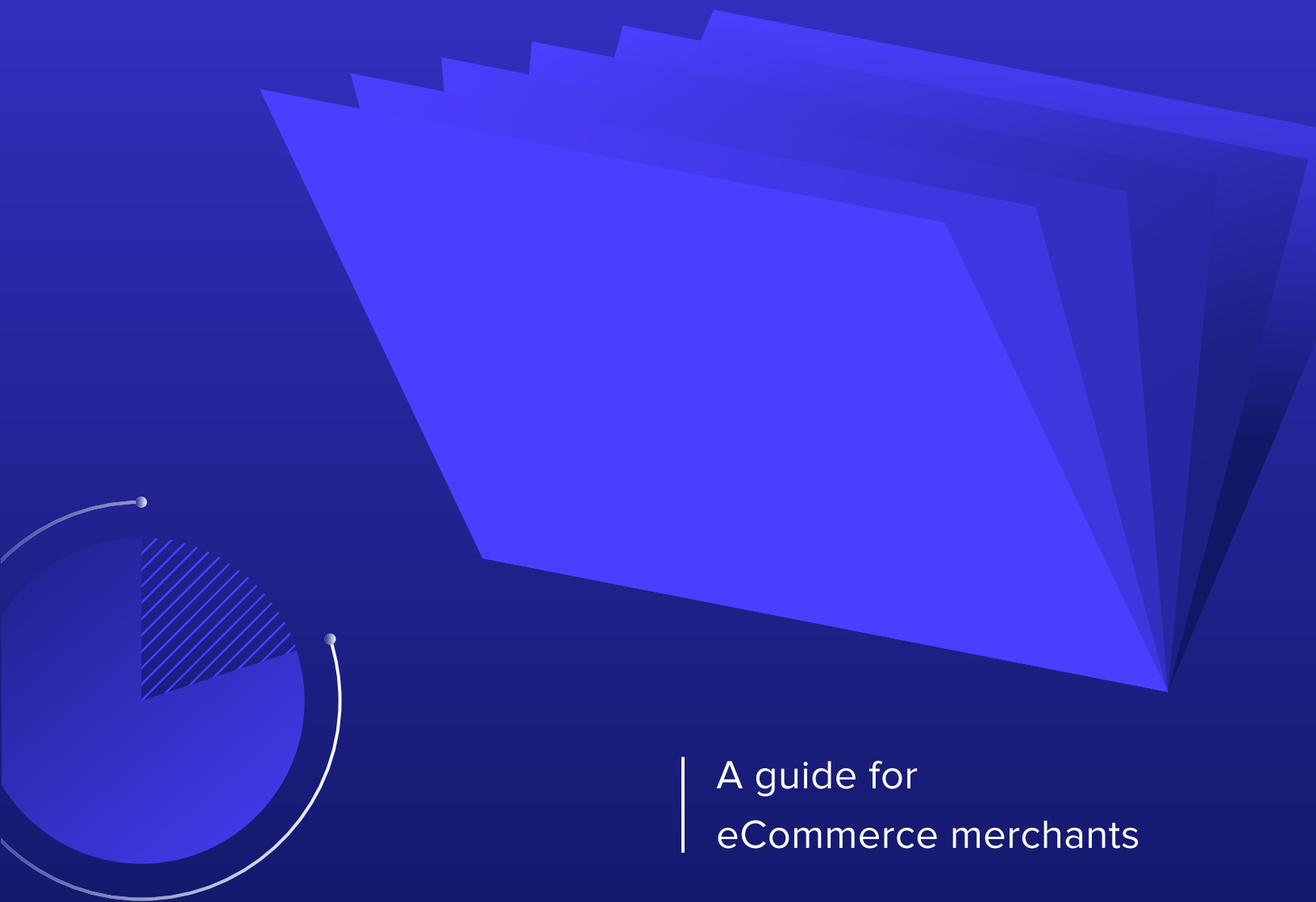
Introducing the **Fraud Management Solution Buyer's Kit**



A guide for eCommerce merchants

Table of contents

Introduction

As the global eCommerce market grows and fraud methodology evolves, new approaches and tools are introduced at a fast pace. Trying to stay on top of developments in the eCommerce fraud prevention landscape can be overwhelming and time consuming. Riskified is proud to present the eCommerce Fraud Solution Buyer's Kit, a comprehensive series of resources designed to guide executives and procurement professionals through the process of assessing current fraud management performance and understanding which available approaches and solutions can best optimize performance.

The kit includes the following resources:

CNP Fraud Lexicon

- Commonly used fraud terms
- Precise definitions of KPIs
- Explanation of industry jargon

Assessing Current Performance

- Which metrics and KPIs are important
- Who in the organization has this data
- How to benchmark your performance

Approaches to Fraud Prevention

- Overview of approaches to fraud management
- Advantages and challenges of every approach
- What resources are required for successful performance

Choosing a Fraud Management Solution

- What considerations are key to procurement

- How to select the right solution for your organization
- What to focus on when choosing a partner

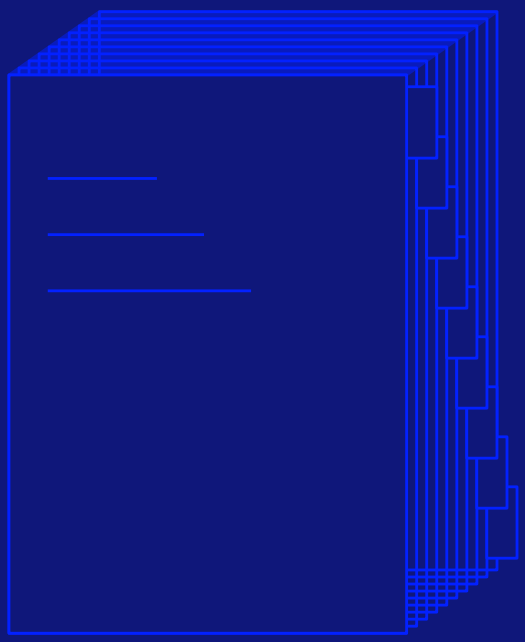
Publishing an RFP for a Fraud Management Solution

- How to conduct an efficient and precise RFP process
- Approaches to publishing a tender overview
- An editable list of sample RFP questions

We hope our kit can provide guidance and insight to streamline your process. Should you have any questions about the kit or anything else, feel free to shoot us an email: sales@riskified.com

For more information: www.riskified.com

From Account Takeover to Whitelist: **The CNP Fraud Lexicon**



Introduction

Fraud detection is a science, and mastering the subtleties of the field means getting familiar with its terms and vocabulary. Whether you're searching for a third-party fraud solution, evaluating the performance of your in-house team, or just getting acquainted with the ins and outs of CNP fraud, you're likely encountering industry jargon, which can be difficult to decipher.

With this in mind, we've created this lexicon as a guide for merchants, to elucidate some of the most commonly used fraud terminology.

Account Takeover (ATO)

This is a form of sophisticated fraud in which fraudsters gain access to a legit customer's credentials–usually as a result of a data breach–and use them to order goods. Because the fraudster was able to log in to the eCommerce merchant's site, these attacks are particularly difficult to detect. ATOs can take many forms, but the most common methods identified by RIskified are Loyalty Fraud, and "Mismatched ATO". For more information on ATO attacks, check out our guide on the topic here.

Anomaly Detection (aka Outlier Detection)

This term generally refers to the identification of items, events, or observations which do not conform to an expected pattern or other items in a dataset. In fraud prevention, anomaly detection is used to spot unusual shopping patterns that may indicate fraudulent activity. Riskified automatically analyzes all transactional data cohesively on an ongoing basis to identify fraud rings attacks in real-time. Our in-house experts investigate the statistically significant anomalies to determine if they are indicative of a fraud ring attack, fraud bots, or simply reflect an inherent shift in eCommerce trends.

Approval Rate

The approval rate is the percentage of approved transactions out of the total order volume over a given time period. (Riskified measures transaction volume and approval rates in terms of revenue, rather than in terms of transaction count)

AVS (Address Verification System)

One of the first mechanisms devised by payment processors to verify the identity of credit card holders in CNP transactions. Under this system, the zip code and numerical part of the street address provided by the shopper are compared to the corresponding data on file with the credit card issuer. The results of this comparison can be AVS Match, Partial Match, or Mismatch. Many payment processors encourage retailers to use AVS results as a fraud filter on the gateway level. Since credit cards issued outside of the US, the UK, and Canada do not support AVS, this system cannot be used to verify the cardholder's identity in most global markets.

AVS Match / Partial Match / Mismatch

An AVS match means that the zip code and numerical street address in the billing address provided by the shopper exactly match those on file with the credit card issuer - supposedly indicating that the shopper is the true owner of the credit card. Partial Match means one of the two provided numbers - either the street number or zip code - match the number on file with the credit card issuer. A Mismatch means neither of the numbers match. Though an AVS mismatch is a potential indicator of fraud, many legitimate orders fail AVS screening for non-fraud related reasons. Similarly, a full or partial AVS match does not rule out the possibility of fraud, as AVS data is often sold alongside other stolen credit card information on the dark web.

Behavioral Analytics

This term generally refers to the field of data analysis that measures users' behavior on web or mobile platforms. Riskified uses this term to refer to analysis conducted on data generated directly from merchants' eCommerce sites and mobile shopping apps using our Storefront Beacon. A twenty minute shopping session can contain thousands of data points, and when these browsing patterns are analysed and cross-checked against millions of other shopping sessions, they become an excellent indicator of the order's fraud risk.

BIN (Bank Identification Number)

The first four to six digits of a credit or debit card. These digits indicate which bank or institution issued the card. For example, if the first six digits of a card are 317207, this means it is an American Express card issued by Delta Skymiles, in the United States.

Bots

Short for software robots, this term is used to describe tools designed to carry out repetitive tasks automatically. Tech savvy fraudsters may deploy bots to target eCommerce websites, by creating fake accounts and placing orders using stolen credit card details. Riskified's systems detect bot activity through order linking and anomaly detection.

Card Testing

A practice employed by fraudsters to check that their stolen credit card details are valid, before attempting a big heist. When testing cards, fraudsters tend to place multiple low-value purchases, in an attempt to 'fly under the radar' and avoid having the orders flagged by fraud scoring tools. Card testing often takes place on the sites of non-profit organizations. These sites are targeted because giving an online donation does not require a shipping address, and because fraudsters know non-profits are unlikely to have sophisticated fraud detection safeguards in place.

Cart Abandonment (Customer Drop-Off)

Cart abandonment, or drop-off, refers to customers who begin the checkout phase on a retailer's website but ultimately drop off or abandon their purchase before completing it. A high cart abandonment rate indicates that merchant investment in customer acquisition is being lost. The main reparable problems that lead to high drop-off rates include a long, complicated checkout process, and friction.

Chargeback

When a customer reports a fraudulent or otherwise unsatisfactory transaction to their credit card issuer, the issuer is legally obligated to refund the charge. The issuer then forwards this cost to the merchant, along with a code and reason for the chargeback. There are various chargeback reasons, including:

item not received; **item defective**; **documentation received was invalid or incomplete**. Merchants who inadvertently approve fraudulent transactions incur chargebacks when the legitimate cardholder realizes that unauthorized purchases were made with his or her card. When merchants fail to identify fraud attempts and surpass a certain chargeback rate, they not only incur costly losses, but are also penalized by being enrolled in a an excessive chargeback program.

Chargeback Rate

The chargeback rate is the percentage of transactions for which chargebacks were incurred out of the total approved order volume in a given time period. The fraudulent chargeback rate is the percentage of transactions for which fraud-related chargebacks were incurred (Riskified measures the chargeback rate in terms of revenue). These two KPIs are crucial for merchants who wish to avoid being enrolled in a credit card issuer's excessive chargeback/risk program.

Chargeback Guarantee

Pioneered by Riskified, the chargeback guarantee is business model under which Riskified assumes liability for every approved order in case of fraud. Since Riskified extends its chargeback guarantee to cover all approvals, merchants using Riskified as their fraud management solution no longer have to worry about fraud-related chargebacks. If an order approved by Riskified turns out to be fraudulent, we reimburse the merchant for the entire chargeback amount within 48 hours.

Chargeback Representment

When a fraudulent chargeback is filed (think Friendly Fraud or Liar Buyer), the merchant may dispute the chargeback in a process called representment, by gathering evidence to prove that the transaction was made by the true cardholder. This can include IP, email, billing and shipping address, proof of communication with the customer, proof of delivery and more. If the evidence submitted is compelling, the issuer may decide to reverse the chargeback and return the funds to the merchant.

CNP (Card Not Present) Fraud

A CNP transaction is one where the merchant is unable to physically examine the credit card, usually when a purchase is conducted via digital channels or over the phone. CNP fraud refers to a CNP transaction conducted without the cardholder's permission. Typically, CNP fraud is perpetrated by criminal elements using stolen credit card details (often acquired on the dark web). Common forms of CNP fraud include account takeover fraud, package rerouting fraud, and friendly fraud (including so-called liar buyers).

Customer Friction

Any merchant activity that slows down or impedes the online sales process. Riskified usually uses this term to refer to fraud prevention measures taken by manual review teams for validation purposes, such as reaching out to customers via sms, email, or phone. Customer friction may also result from requiring shoppers to take cumbersome steps to verify their identity during checkout, like 3-D Secure.

CVV (Card Verification Value)

This is the 3 or 4 digit number printed on the back side of the credit card. The CVV was intended as a safeguard against CNP fraud - since in theory it ensures the shopper has the physical card in their possession. In practice, however, the CVV is usually sold along with the stolen credit card details on the dark web.

Dark Web

The Dark Web is a subset of the Deep Web (Internet content which is not indexed by search engines) that cannot be accessed without specific software or authorization. Although some Dark Web activity is legal, the anonymity it affords makes it a haven for illicit activity. Stolen credit card details sold on the Dark Web include not only the full card number, but also AVS, CVV, and full billing address.

Data Enrichment

Riskified uses this term to refer to the process of supplementing the raw order data collected with additional details that allow our models to accurately assess the order's validity. Riskified's system automatically enriches raw order data with information from proprietary in-house databases, as well as with data from third party sources like Email Age, WhitePages.com, and social networks.

Decline Rate

The decline rate is the percentage of declined transactions out of the total order volume over a given time period. When calculating the decline rate to assess fraud operations performance, merchants should take into account orders rejected due to fraud filters on the gateway level, orders automatically declined by in-house fraud prevention systems, and orders declined by the manual review team.

Device / Browser Fingerprinting

A device or browser fingerprint is information collected about a remote desktop or mobile device for the purpose of identification. Riskified's Storefront Beacon generates this information, and our machine learning models then analyze it along with order data to determine whether the transaction is legitimate or fraudulent.

Disposable Email Account

Many online services allow users to create free email accounts without providing any personal information. These anonymous email accounts can also be easily disabled once they have served their function, hence the moniker "disposable". Fraudsters often utilize disposable email accounts to avoid associating their personal email accounts with their criminal activity.

Email 'Age'

This term refers to how long an email account has existed. The email age is a valuable datapoint when assessing the fraud risk of a CNP order. A recently created email account is much more likely to be associated with fraudulent activity, whereas an order placed with an email created several years ago is a positive indicator of legitimacy. As part of Riskified's automatic data enrichment process, raw order data is often supplemented with email age information.

EMV (Europay, Mastercard and Visa)

A standard for 'smart' cards equipped with computer chips in addition to magnetic stripes, with the aim of authenticating transactions and reducing Point of Sale credit card fraud. Many warned that since EMV makes it more difficult to commit in-store payment fraud, rolling out this technology in the US would drive CNP fraud rates. However, a recent study by Javelin concluded that the recent rise in CNP fraud is not being influenced by the introduction of EMV cards.

Excessive Chargeback/ Risk Program

Merchants who surpass a threshold chargeback rate set by credit card issuers are penalized by enrollment into an Excessive Chargeback/Risk Program. The terms of these programs vary between issuers, and depend on the degree and persistence of high chargeback rates, but most penalties include some combination of fines, higher processing fees, and mandatory risk education programs.

Exposed Fraud

Riskified's term for fraud attempts where the fraudster doesn't attempt to conceal his or her identity. For example, someone purchasing goods online using billing address details from a stolen credit card, but providing their own shipping address.

False Decline

When a retailer mistakenly rejects an order from a legitimate customer due to suspected fraud. False declines may occur for various reasons, including blacklists, fraud filters (such as AVS), data mismatches, or simply that the retailer has insufficient data to confidently approve the transaction. The majority of false declines can be avoided using a combination of data enrichment and machine learning.

Fraud Rate

Riskified defines the fraud rate as the percentage of clear-cut CNP fraud attempts (transactions declined due to clear-cut fraud) plus fraud-related chargebacks, out of the entire order volume, over a given timeframe. For example, if out of $100 worth of online transactions, $1 returns as a fraud-related chargeback and $4 are declined after being identified as a clear-cut fraud attempts, the fraud rate is 5% ($5 out of $100).

Friendly Fraud

When a customer files a fraud-related chargeback, claiming unauthorized card usage, despite the fact that they actually purchased the item. This can happen for several reasons. It can be the result of an honest mistake, like a child using a credit card to place an order without the parents' knowledge, or a shopper not recognizing the transaction on their credit card bill. It may

be a circumstantial case of chargeback policy abuse which wasn't premeditated and is unlikely to repeat itself. For instance, a customer books a hotel room for a trip that is subsequently cancelled. The customer reports unauthorized card usage to avoid paying for a booking that he or she did not benefit from. Finally, friendly fraud can occur as part of a deliberate, malicious plan on the customer's part (aka Liar Buyer).

Fraud Filter

A screening mechanism that rejects orders that fail to meet certain criteria. Fraud filters can be set on the payment gateway level - for example filtering orders with negative AVS match or placed with a card issued in a certain country. Fraud filters can also be applied within the merchant's fraud prevention system, such as the immediate decline of orders above a certain ticket value placed via a device location in a risky geographic region.

IP Address

The IP (Internet Protocol) address is a number assigned to every device that communicates over a computer network. One function of the IP address is that it indicates the geographic location of the computer network. Riskified Storefront Beacon collects IP address data for every online transaction reviewed for fraud directly via the retailer's eCommerce site or mobile shopping app. The IP address can help reveal the customer's location and is taken account along with other data points when determining the potential risk of the transaction. Fraudsters often use proxy servers in an attempt to conceal their IP address (and true location).

Liar Buyer (form of Friendly Fraud)

Also known as Chargeback Fraud, this is a form of theft where cardholders exploit chargeback reimbursement policies. A customer purchases and receives goods or services, but then claims the purchase was unauthorized or that the item was not received. As a result, the retailer incurs a fraud-related chargeback and the customer is reimbursed by the credit card issuers.

Loyalty Fraud

A form of ATO fraud which can occur when there is store credit or rewards cash balance saved in a customer's account, which

fraudsters can use it to shop immediately. The most common examples of this are frequent flyer miles or hotel loyalty points, where it's quite possible that a customer has significant value stored in the account. When a fraudster commits loyalty fraud, the merchant is responsible for reimbursing those stolen points, miles or other store credit.

Machine Learning

An advanced artificial intelligence technique which allows computers to refine their behavior ("learn") without being explicitly programmed. Machine learning-based fraud management solutions have several advantages over rules-based systems. Machine learning models are less rigid than rules, and can continuously self-optimize simply by "learning" based on exposure to new order data. Riskified also leverages feature engineering to enhance the models' accuracy. Rather than providing our models with only raw order data, we engineer features that encapsulate the knowledge and insights our domain experts have about CNP fraud patterns and about the relation between data points.

Manual Review

A process by which analysts manually review orders for fraud, usually after automated fraud detection systems fail to definitively determine whether or not an order is valid. Rather than relying only on statistics, manual fraud review teams make decisions based on judgement and experience. On top of approval rate, and chargeback rate, the effectiveness and efficiency of manual fraud review teams is often measured based on the review turnaround time.

Mismatched ATO

This is the most common ATO pattern that Riskified has identified. In these cases, a fraudster obtains account information, but not the associated credit card details. This attack has a high success rate; Many merchants, unaware of the scope of the ATO issue, decide that good login credentials are enough to essentially auto-approve an order. And even when merchants detect something suspicious in one of these orders, they tend to refrain from requesting additional identity verification steps to verify the identity of this "loyal" customer.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication is an identity verification method in which a user must present two or more pieces of evidence, or factors, in order to access their account or proceed with a transaction. These factors must be from different realms: a knowledge factor (something you know, such as a password); a possession factor (something you have, such as a code sent to your phone); and an inherent factor (something intrinsic, like a fingerprint). MFA adds additional layers of security and makes Account Takeover (ATO) more difficult to carry out. A common implementation of MFA is 3-D Secure.

Negative List (aka Blacklist)

This term refers to records of physical addresses, phone numbers, IP addresses, emails, or credit cards that merchants have identified as being associated with CNP fraud. These records are kept so that new orders containing details that appear on the negative list will be automatically declined. Riskified advises merchants to avoid using negative lists for fraud prevention purposes, as this practice tends to exacerbate the problem of false declines.

Order linking

The practice of cross-checking all data from new transactions against previous orders. Order linking can help prevent fraud, for example, when a new order is placed from a device and IP address from which a fraudulent chargeback was previously incurred. Linking also helps approve orders placed by good customers. For instance, it will allow you to identify legitimate shoppers returning with a different surname (due to marriage), or shipping to a new address. Using order linking, Riskified can help retailers approve orders from first-time shoppers (who previously shopped with other Riskified merchants). It also allows Riskified to easily identify and foil the activity of fraudsters and “liar buyers”.

Package Rerouting

Package rerouting is the practice of changing an item’s delivery address after the purchase has been approved, sometimes after the package has left the warehouse and is already in-transit. Many retailers and shippers offer shoppers the option to change the shipping address after placing an order online. Unfortunately,

this service can be exploited by fraudsters. A classic package rerouting fraud scheme involves placing an order with stolen credit card information, and providing the shipping address associated with the legitimate card holder in order to "trick" the retailer into approving the purchase. Then, once the order has been approved by the retailer, the fraudster reroutes the package to a different delivery address. This type of fraud can be difficult to prevent, because it requires monitoring shipments for aberrant behavior after the purchase has been approved. Merchants can ask the shipping provider to block the rerouting option. Another option is reassessing the order again given the new shipping destination.

Payment Declines

When a bank or other financial entity declines an order during the authorization process. Certain transaction types are more likely to be declined, for example cross-border orders or those placed using foreign payment methods. However, a great number of declined orders are actually valid, keeping good customers who can afford the purchase from completing a transaction.

PII (Personally Identifiable Information)

This term refers to any information which could potentially be used to identify an individual, such as full name, passport number, and so on. Companies holding PII on their servers must comply with government mandated security regulations to safeguard this sensitive information, and for good reason: PII is a very common target for cyberattacks, since possessing this data allows criminals to commit identity theft, and enables fraudsters to better imitate credit card holders, increasing their chances of successfully executing CNP fraud attacks.

Proxy Detection

In the context of CNP transactions, proxy usage refers to cases where rather than browsing a retailer's website directly from the server closest to their device, customers connect to the retailer's site via an additional server. Riskified's proprietary technology allows our systems to accurately determine whether or a proxy server was used while placing an order. While there are many legitimate reasons for using proxy servers, fraudsters often use proxies to conceal their true IP address (and therefore, the geographic location of the device).

PSD2 (Payment Services Directive 2)

The revised Payment Services Directive was adopted by the European Parliament in order to increase security for merchants and consumers in CNP transactions. It mandates that all intra-European transactions be reviewed using one of two different fraud prevention measures. The majority of orders require Strong Customer Authentication (SCA), a two-factor authentication process. Some orders, namely those of lower value and risk, may be exempt from SCA and instead qualify for Transaction Risk Analysis (TRA). TRA is a quick and frictionless process, thereby reducing the risk of drop-off.

Review Turnaround Time

The duration it takes to review an order for fraud and reach a decision as to whether to approve or decline the purchase. High review turnaround times can lead to shipping delays, damaging brand reputation and customer dissatisfaction.

Reshipper

Also known as a reshipping service, freight forwarder, or forwarding agent. A reshipper is a service that acts as a physical intermediary, receiving packages from retailers and then shipping the goods to the end customer. Though there are legitimate reasons to use reshippers, they are also heavily utilized by fraudsters in order to conceal the true shipping destination from the retailer.

Rule-Based System

In the context of CNP fraud management, these systems are used by merchants to set up rules that determine which orders are immediately approved, declined, or challenged - and consequently routed for manual review. For instance, a merchant can set up a rule to automatically decline all orders shipping to high-risk countries, and to automatically approve orders placed by returning customers. Alternatively, rules can be designed to divert all orders with AVS mismatch to manual fraud review. Merchants using rule-based fraud prevention systems usually assign at least one full-time employee to managing and updating the rules. As fraud methods constantly evolve, the rules must be validated and updated on a regular basis to effectively prevent fraud.

Safe Approval Rate

Riskified defines this term as the percentage of approved orders for which fraud-related chargebacks were not incurred, over a given time period. For example, a retailer approves 98% of all CNP transactions. Several of the approved orders are actually fraudulent, and the retailer then incurs fraud-related chargebacks for these orders. Therefore, while the retailer's approval rate is 98%, the safe approval rate is slightly lower, at 96.5%.

Scoring System

In the context of CNP fraud management, a scoring system provides merchants with a 'risk score' for every order. Merchants relying on scoring systems often define rules to determine how to handle orders based on their score. For example, orders below a certain score threshold may be automatically approved, orders with a score above a certain threshold may be immediately declined, and orders with intermediary scores may be routed to manual fraud review. Merchants using scoring systems remain liable for fraud - meaning wrong approvals can generate costly chargebacks.

Social Network Footprint

This refers to the trail of publically available data that social media users inadvertently share when using networks like Facebook, LinkedIn, and Twitter. When possible, Riskified uses the social media footprint to approve orders despite data mismatches, and avoid false declines. This data can also be used as compelling evidence of friendly fraud or liar buyer when disputing a fraud-related chargeback.

VOIP / Virtual Telephone Number

Virtual or VOIP (voice over IP) phone numbers are not directly associated with a landline or mobile phone device. For example, a person living in the US but working with Japanese clients can pay Skype for a Japanese phone number. Incoming calls or messages will be routed to the user's Skype account. Fraudsters use virtual phone numbers to avoid providing their personal phone number. If merchants call the number to verify the buyer's identity, the call is forwarded to the fraudster's real phone.

Web Beacon (Or Storefront Beacon)

A snippet of code embedded in a web page, which tracks the behavior of visitors to that page. Riskified's Storefront Beacon is embedded on the eCommerce sites and mobile shopping apps of merchants using our service. Riskified uses the beacon allows for proxy detection, and device and browser fingerprinting, as well as to gather data about online shopping patterns for behavioral analytics.

Whitelist

This term refers to records of physical addresses, phone numbers, IP addresses, emails, or credit cards that merchants have identified as being associated with legitimate customers. Merchants may choose to automatically approve orders containing whitelisted data as a way to reduce review turnaround times. The downside of relying on positive lists is that, if details of a previously "whitelisted" credit card are stolen and used by a fraudster, the merchant will immediately approve the order, without reviewing it for fraud.

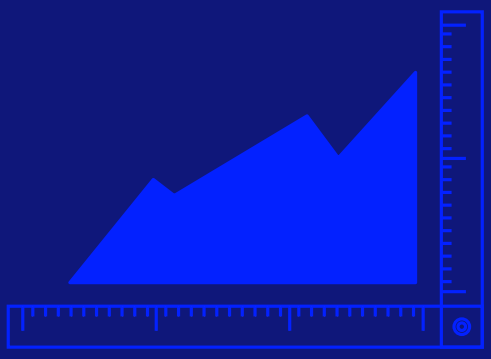
3-D Secure

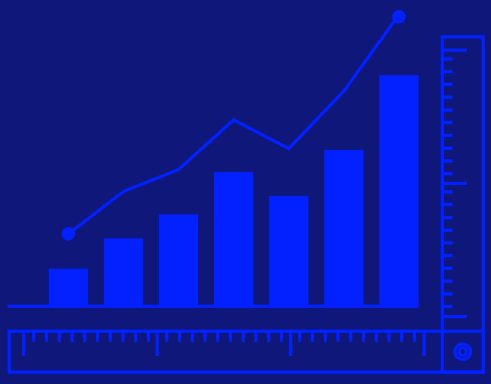
A customer identity validation protocol designed by credit card issuers in an effort to prevent CNP fraud. To complete a purchase, shoppers are required to enter a code provided by their card issuer. Using 3-D Secure shifts fraud liability to the credit card issuer. However, this high-friction measure has been linked to high drop-off rates in key global markets such as the US, China, and Brazil.

We hope this lexicon was helpful in elucidating some of the most commonly used CNP fraud management terms.

To learn more about how Riskified's CNP fraud solution can benefit your eCommerce business, contact sales@riskified.com

How To Assess **Fraud Management Operations**





Introduction

Gauging the cost and effectiveness of your organization's current fraud management process can be tricky. Ownership of fraud management operations is often fragmented, with stakeholders spanning the eCommerce, payments, fraud, IT, customer service, and finance departments. In addition, it's not always clear what opportunities or losses are associated with fraud management, and analyzing data comprehensively is not always simple math. We compiled this document to help clarify which KPIs are important, and which team or department is most likely to have access to the relevant information.

Once you have collected all the metrics, you will be able to better assess your current fraud management performance, as well as identify weaknesses and areas for improvement.

Collecting Key Metrics

Please note: All percentages related to transactions (such as decline rate, chargeback rate, etc.) should be calculated on a revenue basis unless noted otherwise.

High Level Metrics

These are the basic numbers you need to assess overall performance

ECOMMERCE FINANCE	Annual value of CNP orders ($) (desktop, mobile, & phone orders)
ECOMMERCE FINANCE	Average order value ($)
FINANCE	Customer lifetime value ($) *1

Fraud Management Costs

Operational expenses paid annually to support fraud prevention efforts

FINANCE PROCUREMENT	Fraud system and tools costs ($) *2
FINANCE PROCUREMENT	Fraud team salaries ($) *3

Approval Rates

How many of your potential customers are being rejected?

FRAUD PREVENTION, PAYMENT PROCESSOR	Gateway, filters, & rules rejection rate (%) *4
FRAUD PREVENTION	Automatic approval rate (%)
FRAUD PREVENTION	Automatic rejection rate (%)
FRAUD PREVENTION	Manual review rate (%)
FRAUD PREVENTION	Manual rejection rate (%)

Customer Experience

How many of your customers have a sub-par experience?

FRAUD PREVENTION, CUSTOMER SERVICE	Rate of orders held more than an hour in the manual review queue (%)
FRAUD PREVENTION, CUSTOMER SERVICE	Rate of customers contacted for additional information (%)
MARKETING, CUSTOMER SERVICE	Customer insult rate (%) *5
FRAUD PREVENTION, PAYMENTS	Rate of 3D-Secure, if applicable (%) *6
FRAUD PREVENTION, PAYMENTS	3D-Secure drop off rate (%) (% of orders where customer didn't complete 3D secure step and failed to complete purchase)

*1 The customer lifetime value, or LTV, is the projected revenue generated from a customer over their shopping lifespan.There are several ways to calculate a customer's lifetime value.

*2 This includes the cost of purchasing fraud system and tools, as well as any ongoing costs associated with using these tools (e.g., monthly usage fees).

*3 This includes the salary expenditures for the manual review team, as well as the salaries of data scientists, fraud researchers, IT personnel, and any other staffing costs associated with integrating new tools into your system (e.g., Maxmind, Emailage), for the purpose of maintaining and optimizing your risk models or fraud rules.

*4 Orders that were automatically declined due to fraud filters and rules (include only orders where payment was authorized, and exclude hard declines from the payment processor).

*5 How many of your customers file a complaint with customer service or reach out via social media to complain about declined orders, shipping delays, or friction in the shopping process.

*6 3D Secure is a consumer authentication service requiring the customer to provide an additional code in order to continue with the checkout process.

Identifying Weaknesses & Opportunities

After collecting the metrics tied to your organization's fraud management performance, it's time to analyze the stats in order to identify weaknesses and opportunities. As part of this analysis, it's important to determine what characterizes your organization's current fraud prevention strategy. Below are profiles of three common types of eCommerce retailers whose fraud operations are not fully optimized. Every profile includes a synopsis of the situation, as well as the opportunity presented by working to optimize fraud operations. While these profiles are stereotypical, it's worth reading through them to see if any of them seem familiar to you.

1 The exceedingly risk-averse retailer

This retailer has a very low chargeback rate coupled with a high rate of declines. These retailers impose tight controls and strict rules in an effort to block fraudsters. As a result, they often reject many valid transactions along with the fraud attempts. This high rate of false declines makes it difficult to grow your customer base, and lowers your average customer lifetime values.

Opportunity

By optimizing fraud operations you can:

- Increase sales revenue & expand to new markets
- Provide a better customer experience
- Nurture and grow your customer base

2 The overly trusting retailer

The overly trusting retailer has high approval rates and a virtually non-existent fraud process, as fraud has never been a problem. When the business is eventually targeted by fraudsters, this retailer is completely vulnerable. With no fraud strategy, no one dedicated to fraud prevention, and zero mechanisms to deal with fraud and chargebacks, the overly trusting retailer will eventually face a huge reckoning for which they will only have themselves to blame.

Opportunity

By optimizing fraud operations you can:

- Implement a fraud management strategy
- Prepare your business in order to prevent or reduce fraud-related losses
- Avoid being entered into “excessive risk” programs

3 The non-automated retailer

The non-automated retailer has amassed quite a large fraud team. Using basic rules and filters, non-automated retailers usually route a large amount of orders to manual review. Due to heavy reliance on manual work, this type of retailer has a lot of overhead costs, especially around product launches, holidays, and peak sales seasons. These retailers are susceptible to shipping delays and customer dissatisfaction stemming from long order review times.

Opportunity

By optimizing fraud operations you can:

- Reduce the workload on your team
- Improve fulfillment timeframes & avoid shipping delays
- Provide a better customer experience

Benchmarking Your Performance

Benchmarking your fraud performance based on the metrics you’ve collected isn’t always easy. Numbers vary greatly between verticals and markets; for example, selling sneakers online carries more risk than selling other mainstream fashion items and apparel, which in turn carries more risk than selling auto parts. This is why sneaker merchants are likely to experience more fraud attempts and may potentially have higher chargeback rates, while online auto parts merchants can expect significantly lower fraud rates altogether.

To illustrate variations in metrics across verticals, let's compare "ideal" stats: **Mainstream fashion merchants** should strive for a chargeback rate that is near 0.1% of orders (in terms of $ value). They should be approving nearly 99% of orders. **Sporting goods merchants** shoulder more risk. An ideal chargeback rate is near 0.15%, with an approval rate of roughly 98% of orders. Manual review should be minimal, or non-existent in all cases.

Looking only at the performance of another retailer won't necessarily help you understand whether you are doing well. To find numbers that will allow you to accurately benchmark your fraud performance, try:

- Comparing stats with colleagues in your industry, or in a vertical that carries similar risk
- Joining the MRC community and talking with merchants who are facing similar challenges. Every year, the Merchant Risk Council publishes a global fraud survey, which can also help benchmark your performance

Summary and Next Steps

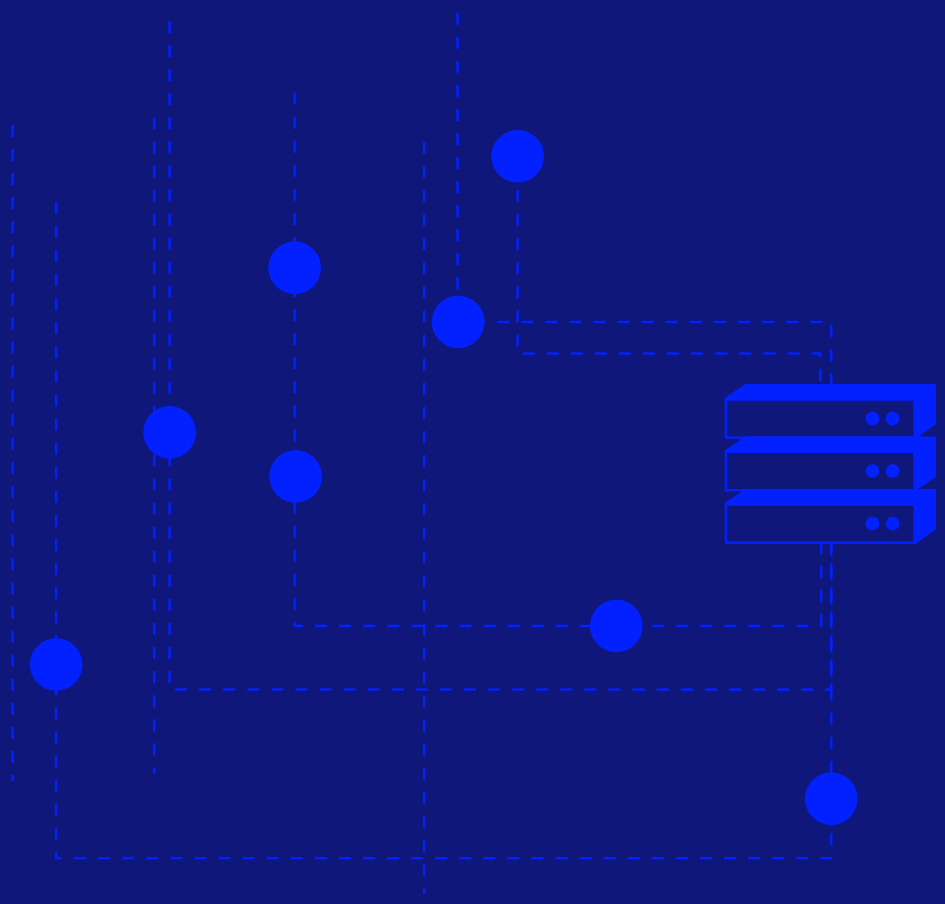
Once you've begun benchmarking your performance, you should be able to start identifying opportunities. Next, prioritize the areas for improvement and decide what you want to focus on:

- Determine which of the areas for improvement are most important for your business
- Establish what problem is holding your business back the most, and what changes will deliver the highest ROI or upside

After the priorities are set, your work is cut out for you. Learn about available solutions, and understand both how they can complement your business today, as well as how they can support your growth strategy.
You are also always welcome to turn to our fraud experts. We'll be glad to assess your performance in relation to your vertical and business case free of charge, and to help identify pain points and opportunities for improvement and growth.

For more information: www.riskified.com | sales@riskified.com

Approaches to Fraud Management



Introduction

The vast majority of eCommerce businesses are either utilizing a fraud management system or are in the process of evaluating one. As the eCommerce markets grows, fraud methodologies evolve, consumer expectations change, and a process or approach that may have served you well so far may not be scalable or flexible enough to meet your business needs. Being aware of the various approaches eCommerce merchants adopt to handle fraud can be an advantage. This document describes the four key approaches merchants take when it comes to eCommerce fraud prevention, and explains the advantages and challenges of every approach.

Common Fraud Management Challenges

When it comes to managing fraud, there are three key challenges faced by all online retailers:

Fraud liability

One of the most obvious and painful challenges of managing online fraud is the liability and potential high cost of mistakes. As it stands, merchants are liable for any online purchases reviewed and approved in-house. Maintaining low chargeback rates is important not only to avoid unexpected losses, but also to stay below chargeback thresholds set by payment processors as to avoid being entered into “excessive risk” programs. Merchants identified as excessively risky pay higher processing fees and are subject to hefty fines for chargebacks, all of which dramatically increase operational costs.

Revenue lost to subpar performance

Most eCommerce merchants do not have extensive development resources and fraud prevention is not their main focus. Quickly identifying sophisticated fraud rings is complicated, and suboptimal performance often results in excessive chargebacks while leaving potential revenue from good customers on the table.

Ongoing investment in fraud operations

Manual review

Most merchants rely on manual review to some extent. But they're incurring high overhead costs, and are in a bind when it comes to scaling up. During sales seasons, they need to either hire seasonal employees or overload the manual review team, resulting in slow processing times. Effectively reviewing orders requires expertise, so in-depth training is needed to maintain the same performance level.

Managing rules engines & case management tools

Merchants who use fraud prevention rules engines and case management tools must invest time and resources in ongoing maintenance. The rules must be updated after every fraud-related chargeback to make sure similar fraud attempts are declined next time. The end result is a complex system with too many rules to maintain.

Keeping up-to-date with multiple tools and data sources

Many merchants use data from third party data providers, such as Ekata, Emailage, and Maxmind, to validate risk or case management scores. Fraud teams within large companies may use ten or more data enrichment and validation tools. This mandates a sound strategy for when and how to use every data source, and to train the team on every new tool.

The Three Approaches to Fraud Management

1. In-House Fraud Management

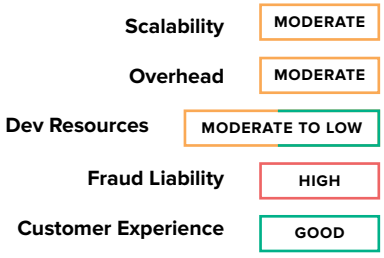
Scalability	POOR
Overhead	HIGH
Dev Resources	HIGH
Fraud Liability	HIGH
Customer Experience	MODERATE

Two types of companies may choose to manage fraud fully in-house: enterprises, and smaller merchants trying to "hack it". Enterprises that manage fraud entirely in-house usually build an internal fraud team and develop their own custom tools. Smaller businesses that manage fraud on their own usually build simple rules along with a developer, and have customer care representatives or fraud team personnel review orders challenged by the rules.

The good and the bad

Managing fraud fully in-house works well for enterprise businesses with extensive resources - as they can achieve good performance while retaining complete control over the entire fraud review process. Most eCommerce companies, however, do not have endless resources to invest in fraud prevention. In the case of merchants who are still relatively small and trying to make it on their own, **trying to manage fraud entirely in-house brings certain pitfalls - most importantly a lack of scalability**. Rapid growth, new product lines or expansion to new markets require adjusting the fraud rules and potentially hiring additional manual review personnel to handle the load. Since fraud prevention is not a core business activity, those tasked with fraud management often have limited access to development and IT resources. The result may be a lack of preparedness for changes in fraud patterns. In addition, a low fraud prevention budget will mean that manual review might be given as a secondary task to employees in the operations, customer service, or eCommerce teams, distracting them from their key goals.time. The end result is a complex system with too many rules to maintain.

2. In-House Fraud Management With External Tools

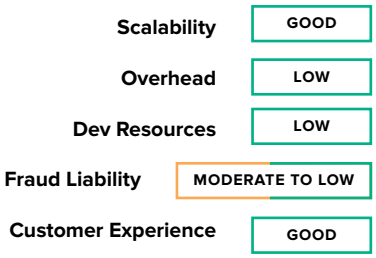


Some retailers with an in-house fraud team use a third-party case management tool that provides a risk score. Based on predetermined rules, the tool approves, declines, or challenges the order, in which case it's routed to further verification. The in-house manual review team has to decide whether to approve or reject the order (sometimes attempting to contact the customer for additional information).

The good and the bad

This approach works well for merchants who have in-house developers and data scientists who can integrate and maintain the case management rules and keep them optimized. The main challenge or pitfall of this approach is that **case management tools require ongoing tweaking and maintenance**. For example, expansion to new markets or introduction of new payment methods on the ecommerce website requires updating the case management rules.

3. Fully Outsourced Fraud Management



Some retailers choose to work with third-party fraud management services to handle all eCommerce orders. An in-house contact person (often the fraud manager) manages the merchant's relationship and day-to-day operations with the third party service provider.

The good and the bad

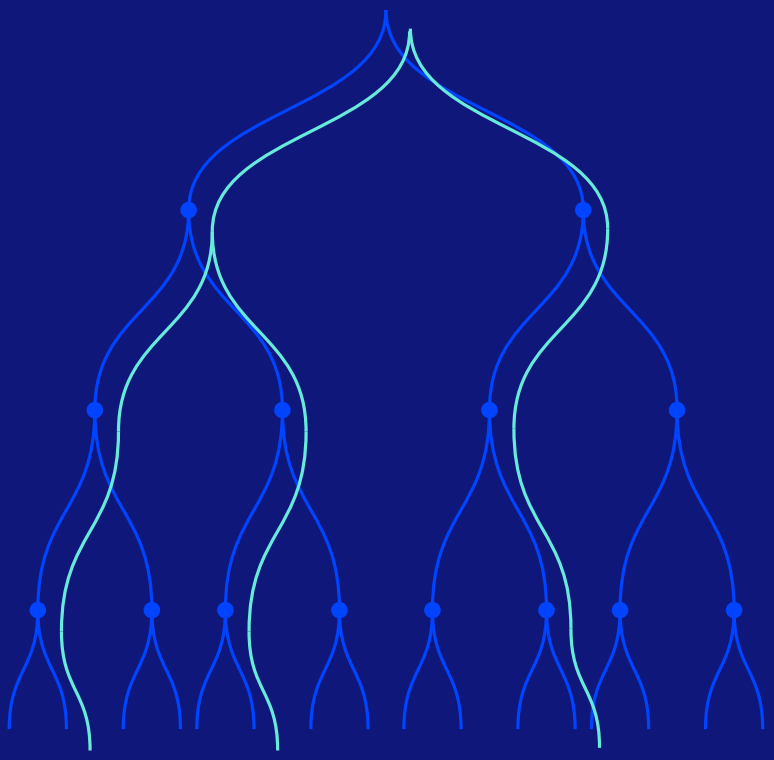
This approach works well for businesses looking to focus on their core business goals rather than invest internal resources in fraud prevention operations. It is especially beneficial for merchants experiencing rapid growth who are reluctant to invest in building an in-house process. It is also a good solution for merchants operating in industries prone to high fraud rates and who are, therefore, also more vulnerable to excessive false positive declines (e.g. travel, gift cards, online event ticket sales). The merchant enjoys complete control over SLA and policy, while letting experts with extensive experience and development resources handle all orders.With a wide variety of tools and systems available, choosing the right third-party solution to best meet your needs, support your growth strategy, and provide the highest ROI can be challenging. As part of this Buyer's Kit, we compiled a list of important factors to consider and key questions to ask when selecting a service provider.

Summary and Next Steps

The purpose of this overview of fraud approaches is to help procurement managers and eCommerce executives identify the best fraud management approach for their organization. We'd be happy to consult you on which approach would best meet your business needs. If you haven't done so yet, we recommend collecting your company's fraud prevention metrics to assess your current performance and identify structural weaknesses & growth opportunities.

For more information: www.riskified.com | sales@riskified.com

Choosing a Fraud Management Solution - **Five Key Questions**



Introduction

One of the greatest challenges faced by eCommerce businesses is choosing the partner that best meets their needs. Asking the right questions is imperative to ensure the solution provider complements your current process and systems, will be able to handle various business flows, and will successfully support your growth strategy. Below are several key questions to consider when embarking on a procurement process for an eCommerce fraud prevention platform:

1 How will the solution impact sales revenue? Is there a performance guarantee?

Eliminating chargebacks is easy if you don't mind rejecting good orders along with the bad. An overly risk-averse solution will reduce both fraud losses and approval rates. A great fraud management solution, however, can not only help you reduce costs and cut losses through improved fraud prevention, but can also add measurable value to your organization - by generating incremental revenue and driving overall performance.

To this end, check whether a fraud management partner can do two important things:

a. Increase your approval rates by approving more orders. This can help recoup revenue from orders that are currently being manually or automatically rejected.
b. Allow you to remove filters and payment restrictions so that more orders may be reviewed and approved.

If a solution provider does not commit to a specific approval rate threshold, you may find yourself with a solution that is declining too many orders in order to minimize risk, leaving potential revenue on the table.

2 What is the pricing model? Who is liable for fraud?

Different fraud management solutions come with different pricing models and guarantees. Generally, traditional solutions, such as rule-based systems (discussed further in the following section) charge a flat fee per transaction, whether approved or declined. New generation solutions charge only for approved orders, meaning it's in your fraud management partner's interest, as well as yours, to approve as many orders as possible.

It's also important to understand where liability for chargebacks lies. With traditional solutions, chargebacks are left up to the responsibility of the merchant, whereas new generation solutions often offer a "chargeback guarantee". The fraud management partners who offer these solutions will reimburse the merchant for any fraud-related chargeback. While the price point for new generation fraud solutions is typically higher, merchants are also receiving more value, in the form of chargeback assurance and higher approval rates.

3 What technology is at the base of the third party solution?

Understanding what approach or technology is at the base of the solution is important because it can impact ramp up time, determine the need for ongoing maintenance and investment on your part, and have implications for the solution's overall performance. Three common types of fraud management tools or solutions are:

a. **Rule-based systems:**
   Rule-based fraud prevention systems analyze various factors - such as billing-shipping distance, AVS match, CVV information - and generate a score for every data point. Based on these individual scores, the system creates an aggregate risk score for the transaction. Businesses relying on rule-based systems can determine the score threshold for a transaction's automatic approval or decline, as well as the range of scores that send orders for manual review. These systems can help automate some of the fraud review process and reduce the manual review load, but ultimately they leave you with orders requiring further review. In terms of overhead, it's important to understand that these systems require ongoing maintenance: the rules must be constantly adjusted based on performance (e.g. if a chargeback was received, you want to make sure the rules know to identify the risk factors next time round); the thresholds for approval and

manual review must also be adjusted based on order volume (e.g. during peak sales seasons you can't route the same rate of orders to manual review).

b. **Fraud filters:**
As opposed to sets of rules that consider many data points, filters tend to be simple and require little maintenance. Fraud filters are often set on the payment gateway, meaning you do not "know" or "see" the transactions they are blocking. For example, filters can be used to block all orders with an international IP address, all transactions where a proxy server has been identified, or all orders placed with a certain payment method. Fraud filters act as bouncers - blocking out entire populations of potentially risky orders. They are effective if you want to avoid accepting purchases from entire segments. But in today's global market, most eCommerce merchants strive to grow their business, and new markets, payment methods, and channels can drive this growth. Filters provide peace of mind in the sense that they block "problematic transactions", but this is also their weakness - they block a great deal of good transactions, consequently curbing sales revenue. Blindly turning away customers may help reduce chargeback rates in the short-term, but can have severe impact on your sales revenue, both immediately and in the long-term.

c. **Machine learning models:**
Machine learning models are a technologically advanced approach to managing fraud. Rather than focusing on individual data points, such as whether or not an order was placed from a specific country, models take into account a combination of parameters to establish a scenario. They then match it with large databases of information in an attempt to determine which scenario is more plausible - that the order is a fraud attempt or that it is a legitimate purchase. As a result, models are typically more granular than rules or filters. A key advantage of machine learning is that with the right setup, the models optimize themselves and require no maintenance or adjustments on the merchant's part. However, machine learning is not a silver bullet. The model's performance relies heavily on learning from past experience, which in turn, requires accurate tagging of clear cut fraud attempts, safely approved transactions, fraud-related chargebacks, and transactions that were wrongly declined. Inaccurate or incomplete tagging of the orders quickly degrades the performance of the entire system. For example, if a legitimate order is wrongly tagged as a fraud attempt, the models will learn to identify similar transactions as fraud attempts - resulting in false declines. If you are interested in a machine learning-based solution, be sure to ask who is

responsible for tagging the data on which the models are trained, and what is done to ensure the accuracy of this tagging.

Another consideration is transparency. Many fraud management solutions operate as a “black box”, without providing reasons for their decisions or scores. Some, on the other hand, provide insight into their decisions and underlying data to clarify the reasons for declines and help merchants strategize, if required. This is particularly useful for customer support and fraud teams, who often need to understand why a specific order was approved, declined or challenged.

In addition to conducting fraud review at checkout, some solution providers offer additional services to manage other aspects of the eCommerce funnel. These may include protection against account takeover (ATO) attacks; representment to recoup lost revenue from fraudulent chargebacks; alternative payment methods to minimize losses from bank declines, and more. It’s important to have a clear understanding of your pain points in order to partner with a provider who can compliment your services and raise performance throughout your shopping and payment funnel.

4 What is the solution provider’s track record?

There are unique fraud MOs and specific risk factors associated with every online vertical, market, product line, and business flow. Merchants selling digital goods, for example, face fraud-related challenges that differ from online travel agents or fashion brands. Ask your potential risk management partner about their track record with and insight into the vertical or industries in which you operate. It’s also important to learn about their experience handling transactions from markets and regions in which you currently operate and to which you aim to expand your reach. Will they be able to achieve a high level of performance in these markets, allowing you to grow your international customer base? Are they familiar with local shopping patterns, payment methods and fraud MOs?

Choosing a partner with a track record that doesn’t match your business goals can be harmful to your business. Ask for referrals from merchants in your market and vertical, or merchants who faced issues or challenges similar to what you are experiencing. Remember - a relevant track record reflects not only the solution provider’s experience and knowledge, but may also allow you to benefit from a network effect. Some solution providers link every order entering their system with vast databases

of previous orders placed across verticals and geographies. This network effect can drive sales for your business by allowing you to approve first-time customers who have legitimate order histories from other merchants.

5 How will the fraud review process impact customers' shopping experience?

Maintaining a pleasant and smooth shopping experience in a brick-and-mortar store is not always easy, but providing a great experience to online shoppers is even more challenging. Since you cannot be physically present to help resolve issues when an order is placed, providing a straightforward, frictionless shopping experience is crucial. When selecting a risk management partner, it's important to make sure you are aware of the potential impact of the fraud review process on the customer experience:

a. **False Positive Declines:**
   Merchants who turn away a good customer due to suspected fraud pay a high price. Over 50% of customers who experience a false decline limit or entirely stop shopping with the declining merchant, so you lose not only the sale but also the lifetime value of the customer. Ask the potential partner to explain how they will minimize false declines, as well as their track record helping merchants handle this issue.

b. **SLA Requirements:**
   Turnaround time is one of the measurable performance indicators for a fraud management solution. How long does it take until a decision to approve or decline an order is made? Solutions that require you to rely heavily on manual review can result in overload on your team during product launches or sales seasons - potentially leading to backlogs and shipping delays. Make sure your fraud management partner can commit to a review time SLA that meets all of your requirements.

c. **Customer Friction:**
   Many merchants reach out to customers for additional information as part of the order validation process. This is not only time-consuming and tedious for the teams, it is also a high-friction measure that degrades the customer's shopping experience.

Calling or emailing a customer to ascertain their identity can be perceived as insulting or intrusive. People buy online in order to save time and effort, so reaching accurate decisions without actively engaging consumers is best practice. Ask fraud management partners how they can make accurate decisions without adding friction to customers' shopping experience.

d. **Omnichannel Shopping Options:**
Savvy consumers demand and expect a multitude of options when shopping online. To remain competitive, merchants must offer same day shipping, in-store pickup, VIP sales, digital gift cards, international shipping, and more. Every one of these options carries unique risks and is associated with different fraud MOs, so it's important to ask about the solution provider's experience handling omnichannel business flows - those you currently offer, and those you plan to offer in the future.

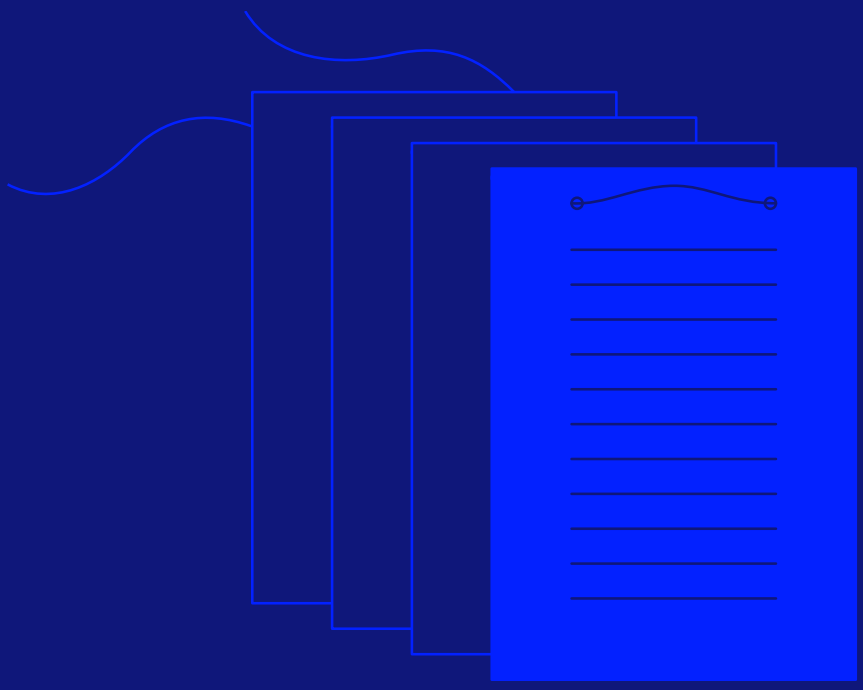
Due to the highly competitive eCommerce landscape, it's imperative to select a solution that will not compromise any of these four elements of customer experience. Many shoppers may be simultaneously browsing your site and your competitors' sites, so the ability to provide a better experience and more convenient options can help tip the scales in your favour. When choosing a fraud management solution, keep your customer's needs and priorities in mind, as fraud prevention measures can impact your ability to grow and maintain a loyal customer base.

Summary and Next Steps

The purpose of these questions is to help ensure you ask the right questions and consider the various ways in which fraud management solutions impact your business as a whole. Knowing these ins-and-outs, along with properly assessing your current performance and becoming familiar with the various approaches to fraud management, will allow you to determine the best fit for your organization.

For more information: www.riskified.com | sales@riskified.com

Publishing an **eCommerce Fraud Solution RFP**



Introduction

This resource aims to assist you in preparing for and managing the Request For Proposal (RFP) stage of your eCommerce fraud solution procurement process. It covers the goals and benefits of publishing an RFP document, includes guidelines for publishing an RFP, touches on key considerations to take into account during the RFP process, and provides sample questions taken from real eCommerce fraud management RFPs.

Goals and Benefits of Publishing an RFP

The RFP is a critical stage in the procurement process, and you should approach it with two clear objectives in mind. The first and more obvious objective is finding the best partner or solution to meet your organization's needs and requirements. To this end, it's important that the RFP document convey any concerns, goals, and expectations you may have from potential partners.
The second and less obvious objective is to help garner the support of executives who don't always understand the complexity and benefits of proper fraud management. Involving all relevant parties in the procurement process will provide stakeholders with insight into the strengths, weaknesses and possible shortfalls of your current process or solution.

Before you start working on an RFP, you'll need to assess your current fraud review process and understand what KPIs are most important for your organization.

Publishing an RFP

A well planned RFP process allows you to procure a service or product that is compatible with your organization and delivers results that meet your specific requirements. When an RFP is hastily put together, the process can leave you confused, or even worse, with a product or service that does not meet your organization's needs.

An effective RFP document should clearly reflect your organization's expectations in terms of performance, results, and overall fit with your various business workflows. For example, if your goals are to generate new growth, scale your operations, or streamline the fraud review process, this should be clearly reflected in the specifications and the questions you ask. Some key considerations to keep in mind:

RFP Length

Keep your RFP document clear, concise, and to the point. Long-winded RFP documents lead to tedious and confusing response documents. Get the information you want by asking clear questions and demanding to-the-point responses.

RFP Scope

Be sure to address the entire order workflow within the RFP document, and to touch on all areas of your operations that may be impacted by changes to your fraud review process or systems. This would include, but would not necessarily be limited to:

- Finance (ROI, payments and capturing funds, chargebacks)
- Customer Relations (customer friction, customer insult rate)
- Fulfillment (automation, impact on warehouse communications)
- IT (required ongoing involvement, support during integration)

Inclusive vs. Exclusive RFP

Will your process be open to various types of eCommerce fraud solutions, or do you prefer to limit your focus to specific types of solutions or vendors? For example, will you only consider solutions that provide risk scores, only consider solutions that provide final decisions, or both? Will you rule out solutions that don't offer chargeback assurance?

You can target specific vendors, open the RFP to all third party solution providers, or determine specific pre-requisites to participating in the RFP process. Narrowing down the field off the bat can save a lot of work down the line.

Rigid vs. Flexible RFP

The best format for an RFP document is a much contested issue. Some prefer rigid templates that require solution providers to answer questions in a fixed way, such as locked spreadsheets where the answers are automatically scored. Other RFP formats give respondents more freedom, allowing vendors to use as many words or lines necessary to answer every question.

The most effective RFP format probably lies somewhere in the middle. Let your respondents make their case where appropriate, but make it clear when you're expecting a simple Yes/No answer. Feel free to limit the length of answers to avoid receiving long and confusing responses. Some enterprise companies opt for 3rd party procurement software solutions to oversee the RFP publications and submission process. These solutions can be configured to be as rigid or flexible as you like.

Make sure to be clear about your expectations, so that vendors responding to your RFP understand what they are expected to provide.

RFP Submission Format

Make it abundantly clear how you'd like potential vendors to submit their response to your RFP. Email? Hard copy? Uploaded via a 3rd party platform? Choose a submission format that will not only be convenient for you to review, but that will also enable you to easily share the submission with others within your organization.

Sample Questions from Fraud Solution RFPs

The following section contains sample questions collected from multiple, real-life eCommerce fraud solution RFP documents. You are welcome to use these sample questions as a basis for your own fraud solution RFP document. For your convenience, these questions are also available in an editable format, allowing you to easily adjust the questions in accordance with your organization's goals and needs.

Solution Overview

- Please provide a brief overview of your company, including size, areas of business, affiliates.
- Please provide a brief overview of your eCommerce fraud solution.
- Please describe your company's experience providing this solution to customers in a similar industry and of a comparable size.
- How will your solution enhance our customer experience and service?
- What sets your solution apart from competitors?

Order Workflow & Review

- What approach does your solution use when reviewing orders for fraud?
- Is there a minimal dataset required for fraud review?
- What data points are scrutinized when reviewing orders for fraud?
- Is your solution fully automated?
- Can your solution review all orders? Can it review specific flagged orders? (challenged/declined/international)
- Does your solution provide a review time guarantee?
- Does your solution provide a chargeback guarantee?
- Are there any payment methods, currencies, or countries that you do not support?
- Does your solution support orders from all CNP transactions? (Desktop/Mobile/Phone)
- Does your solution support expedited/same day shipping, and buy online pickup in-store?

- Does your solution support gift cards (digital/physical)?
- How does your solution interact with our systems to ensure streamlined operations following fraud review? (e.g. fulfillment of approved orders and cancellation of declined orders)
- Will your solution allow us to override or review your decisions?
- Does your solution provide us with reasons for declined transactions?

Fraud Detection & Technology

- Does your solution automatically approve returning shoppers?
- Does your solution use blacklists?
- Does your solution allow merchants to tag for fraud? If so, how do you ensure that mislabeling does not trickle down?
- What is your solution for account takeover?
- Can your solution preempt fraud attacks? If so, how?
- Does your solution use device fingerprinting? 3rd party or proprietary?
- Does your solution track IP address/geolocation/proxy usage? Is tracking provided by a 3rd party or proprietary?
- Does your solution use behavioral analytics to detect fraud?
- Is your solution based on machine learning?

User Interface, Data Review and Reporting

- Describe your graphic user interface; allude to drill down possibilities, performance tracking, and search capabilities.
- Does your solution include automated, real-time reporting?
- What are the management tools available to analyze daily performance?
- What types of performance metrics does your solution measure?
- Are your reports configurable? Are timeframes adjustable to display daily, weekly, monthly, quarterly, and annual trends?

Data Security

- Describe any data (e.g. PII) that you currently or may potentially analyze, collect, manipulate, process, or store.
- Do you transmit, collect, process or store PCI-related data?
- How do you secure our customers' data?
- Please provide a brief description of your Incident Response plan.
- Describe all cryptographic technologies used to protect data.
- Please describe all use of unencrypted communications used in your system.
- What network restrictions do you have in-place to prevent public access to your systems? (e.g. firewalls, proxies, IDS)
- How do you physically secure the resources in which the information will reside?
- Describe the security measures used to prevent unauthorized user access to the data.
- What external assessments and certifications do have you or have you undergone? (e.g. SOC2, ISO, SSAE15, PCI)

System Availability

- What are your backup and business continuity capabilities and procedures?
- Describe your "hot-site" backup capabilities in case of a complete site failure. How often are they tested?
- What is your annual uptime rate?
- What is the expected down time (minutes, hours, day) while the "hot site" is brought up?
- How long does the average call to/from your service take?

Integration & Training

- Please provide an overview of your integration methodology.
- What system integration is required to implement your solution?
- Are there minimal hardware and/or software requirements to run your solution?
- How long is the integration process? Please provide milestones.

- What is the required level of effort by the client during implementation?
- What resources are required to maintain the solution after go live?
- What training is required to operate your solution?
- Is training provided on-site?
- Will you provide supplemental training in case of personnel changes?
- What are the costs associated with standard training?
- What are the costs associated with supplemental post-implementation training, if needed?

Support

- Who on your part will guide and oversee the integration process?
- What kind of support will you provide during the integration process?
- Please detail the technical support packages you provide after implementation.
- What is the availability and response time for client inquiries?
- Are there any costs associated with post-implementation support?

Pricing

- Please provide an overview of your pricing proposal & pricing model. (e.g. do you charge a fee per transaction?)
- Are there any periodical licensing or maintenance fees?

References

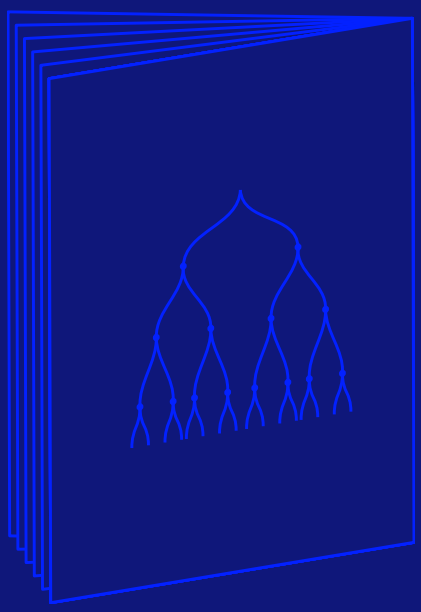
- Please provide references from customers of similar size and vertical.

Reviewing the Responses and Next Steps

Once the RFP process is complete, you'll be busy reviewing and assessing the responses you received. Hopefully, you should narrow down your search to just one or two solution providers. Inviting finalists for face-to-face meetings is best practice. This will allow the vendor to explain the key components and benefits of their solution to stakeholders within your organization, and to address any questions or concerns that may arise.

Be sure to ask vendors to address any specific issues that may have not come across clearly in the tender. Ultimately, a meeting in person is a great opportunity to get a sense of the organization with whom you'll be partnering and hopefully building a long term business relationship.

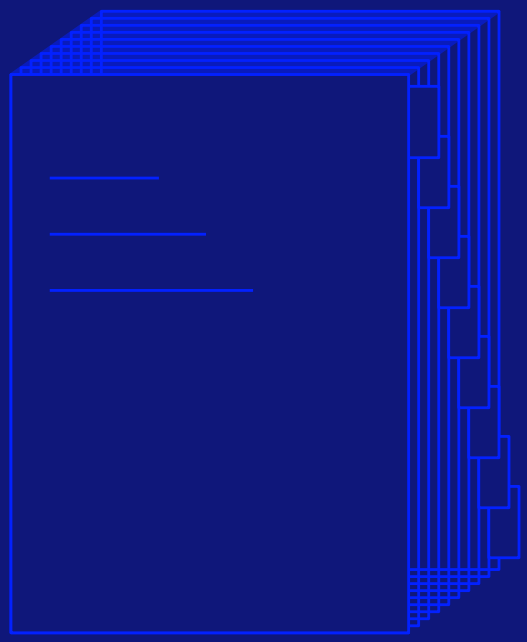
The Riskified team wishes you a successful and fruitful procurement process.



riskified

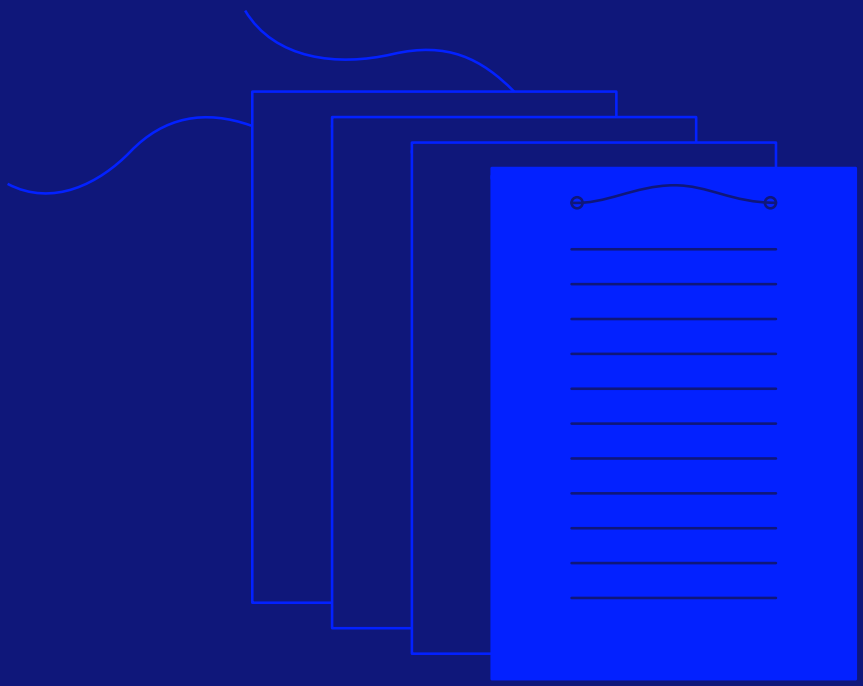
riskified

From Account Takeover to Whitelist: **The CNP Fraud Lexicon**



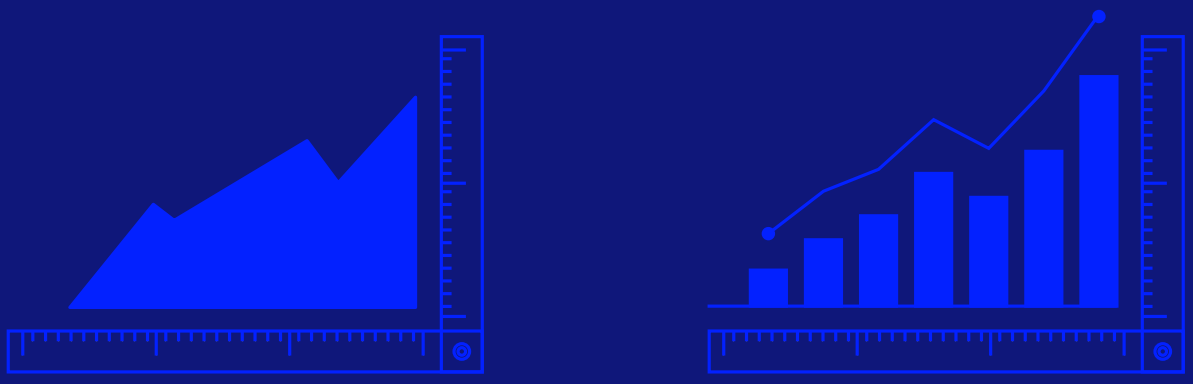
riskified

Publishing an **eCommerce Fraud Solution RFP**



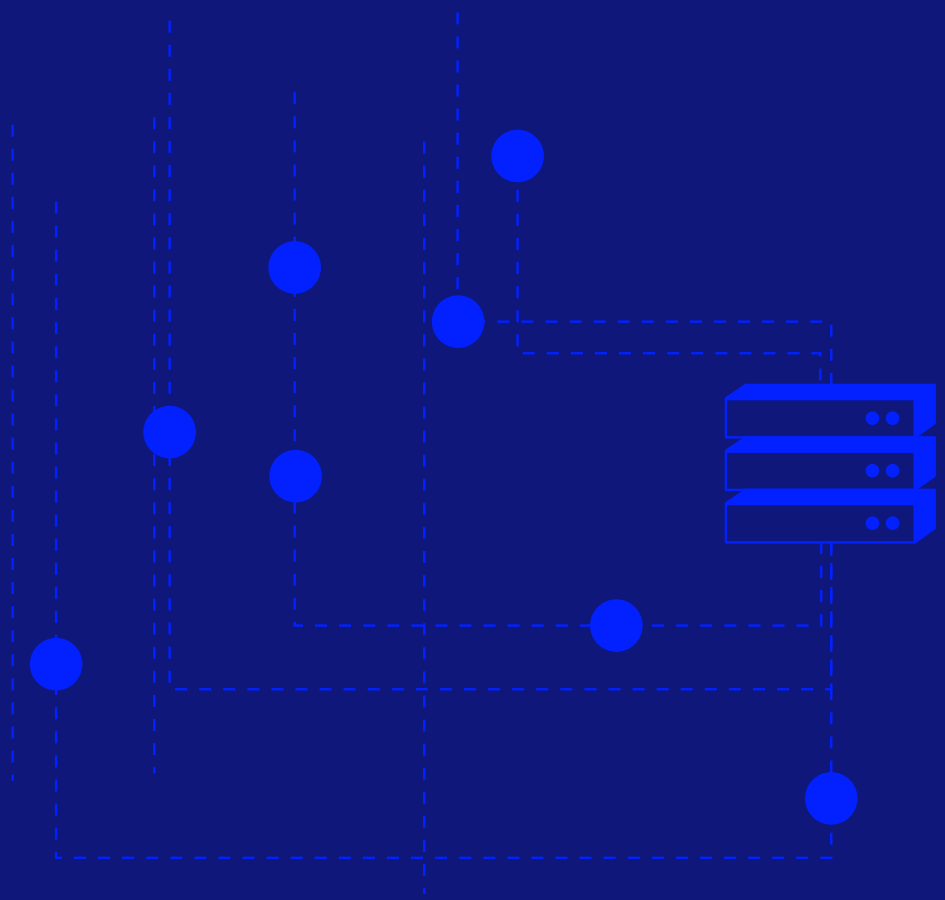
riskified

How To Assess **Fraud Management Operations**



riskified

Approaches to Fraud Management



riskified

Choosing a Fraud Management Solution - **Five Key Questions**