THEFRAUDPRACTICE
PROTECTING THE BOTTOMLINE

connect to address 192.168.1.10
username: **********
password: ************
Access granted...
exited after 0.006146 seconds with return value
any key to continue . . .

PAYMENT FRAUD PREVENTION:
QUICK PIVOTS AND PROACTIVE PLANNING

White paper presented by The Fraud Practice

PAYMENT FRAUD PREVENTION:
QUICK PIVOTS AND PROACTIVE PLANNING

Written by: Justin McDonald, Sr. Risk Management Consultant

A white paper by The Fraud Practice

Sponsored by Sift

Introduction

It's not a matter of ***if***, but ***when***. Fraud attacks ***will*** occur and payment fraud tends to cause the most direct harm and financial damage to both businesses and consumers. Despite acknowledging its severity and near ubiquity, and all of the efforts focused on thwarting it, payment fraud persists as a major industry problem.

Across Sift Network Data, B2C merchants selling digital goods and services saw a 64 percent increase in payment fraud in 2022 while fraud against BNPL increased by 211 percent.[1]

Payment fraud attacks span a wide variety of industries and payment methods. Across Sift Network Data, business-to-consumer merchants selling digital goods and services saw a 64 percent increase in fraud attacks from 2021 to 2022. Sift Network Data[1] additionally showed a 13 percent increase in fraud attacks targeting FinTech and a 211 percent increase against Buy Now Pay Later (BNPL).

Payment fraud causes direct financial losses that have the potential to grow to exorbitant levels and even threaten a merchant's ability to accept payment cards in digital channels. Once fraudsters find a way to steal and make money, they will keep exploiting the vulnerability until the organization can effectively put a stop to it.

Cumulative merchant losses to online payment fraud between 2023 and 2027 will exceed $343 billion globally, according to Juniper Research.[2]

This means continued fraudulent use of payment methods to steal from an organization, which may not show up as a chargeback until weeks later. Beyond the direct financial losses, organizations also suffer from brand abandonment and the loss of lifetime value (LTV) from otherwise loyal customers.

When it comes to combating payment fraud, organizations need to consider both the short-term need to respond to and contain payment fraud attacks as they arise, and their long-term strategy to continue to detect and prevent payment fraud into the future. When a payment fraud attack inevitably appears, the focus shifts to quickly containing it. This aspect of a fraud prevention strategy is the ability to recognize when a quick pivot is needed, and the ability to implement the necessary changes to stop the hemorrhaging caused by an on-going fraud attack.

Sources:

1 - https://resources.sift.com/ebook/q1-2023-digital-trust-safety-index-payment-fraud/

2 - https://www.juniperresearch.com/pressreleases/online-payment-fraud-losses-to-exceed-343bn

An organization's ability to contain fraud attacks with these quick pivots is related to the operational and tactical aspects of managing payment fraud risk, but an effective fraud prevention strategy doesn't end there. An organization must also consider their long-term approach to payment fraud prevention – not just the incremental changes to respond to fraud attacks, but the long-term decisions to ensure their fraud strategy leverages the relevant technology and approaches for fighting fraud. Fraud strategies must evolve over time with broader industry technology and capabilities, as fraudsters will move on to targets with less capability to stop them. This aspect of maintaining a fraud prevention strategy requires proactive planning.

The intent of this white paper is to help organizations examine their payment fraud prevention from both of these perspectives: the ability to implement quick pivots in the face of new fraud attacks, and acknowledging the need for long-run evolutions in the strategy via proactive planning.

This can be applied to what organizations are managing in-house as well as where they lean on their fraud solution partners for assistance. This dual-perspective approach is valuable whether evaluating current or prospective fraud solution providers. Consider not just how fraud solution providers will help with the problems seen today, but how they will help the fraud prevention strategy evolve to keep pace with the ever-changing nature, and increasing sophistication, of fraud attacks.

Payment Fraud Prevention — Quick Pivots

Often, the immediate fix to a fraud attack is a short-term solution. Think of this as triage or first aid – what needs to be done immediately to contain the attack at hand. This may be very specific, such as adding data points to a negative list or increasing the weighted risk of specific products or SKUs targeted by a fraud attack.

There are three primary steps to executing a quick pivot:

1. Recognize the attack and it's characteristics.
2. Determine how to stop it.
3. Implement the changes required to effectively stop it.

Consistent reporting and data analysis can lead to incremental improvements that are proactive, not just reactionary.

Beyond a reactionary response to each fraud attack, organizations should maintain incremental changes in response to new patterns or trends that haven't yet manifested as a full-blown fraud attack. While there is a tendency to think of quick pivots as immediate reactions, there is deep value in regular data reporting and analysis that drives incremental changes in short- to medium-term time horizons as well.

Consider standardized reporting and analysis procedures that encourage transaction and post-transaction data review. These procedures lead to incremental changes when the need for such a change is uncovered. While a pivot may not always be required, there should be varying levels of reporting that have the potential to drive these changes which occur weekly, monthly and quarterly.

This is critical when considering that many fraud attacks focus on reverse engineering and testing different approaches, before the fraudster ramps up their activity to a *"bust-out" attack*. Regular reporting and the resulting minor adjustments can provide improvements beyond fraud detection, such as by improving sales conversion through the recognition of rules or model features that were implicating good users or transactions.

Bust-out attacks refer to when fraudsters first test the waters with low-dollar orders while attempting to reverse engineer a merchant's fraud screening tactics, then launch a large-scale attack with high attempt volume in a short period of time.

Capabilities to support immediate, reactionary quick pivots are necessary, since organizations can't predict every attack. However, with regular data review and incremental model or rule changes, organizations can identify new and growing issues before they become large losses. Managing an organizational fraud prevention strategy includes determining who is focused on the day-to-day fraud management operations to manage these incremental changes in the immediate-, short- and medium-run. Define who these people will be, including the teams, roles and responsibilities, as well as performance metrics for measuring success and defining standards for accountability.

While the ability to quickly pivot is an essential component of any fraud prevention strategy, it's only half the battle. If an organization only makes short-term fixes, eventually the fraud architecture becomes a legacy platform, and the ability to limit and contain new fraud attacks wanes. If organizations reach a point where the fraud prevention, technology tools and platform have become a limiting factor in their ability to respond to the latest fraud attacks, it's already too late. The effort and time it takes to evolve a fraud prevention strategy is extensive, and these large-scale changes must be managed proactively – before they are allowed to become a point of failure.

If an organization fails to evolve its strategy due to a lack of long-run proactive planning, the quick pivots and operational adjustments will lose effectiveness. This may result in the organization's inability to stop a new fraud attack without causing either a detrimental impact on sales conversion or operational strain. This could lead to relying on broad-scope automated responses that turn away good orders or users, or more transactions must be funneled to manual review. Considering the large-scale nature of many fraud attacks, it is unrealistic to expect manual review analysts to keep up. If an organization reaches this stage, it is likely that both operational efficiency and sales conversion will be adversely impacted.

According to Sift surveys, 74 percent of consumers would stop engaging with a brand due to fraud.

Payment Fraud Prevention — Proactive Planning

Whereas quick pivots rely on larger operational teams of managers and analysts, proactive planning focuses on a long-term strategic approach with executive decisions led by the person who owns the fraud prevention strategy and their close-knit team of senior managers. Rather than frequent, incremental changes that solve specific issues, proactive planning focuses on large-scale changes that occur infrequently and typically take several quarters, if not a year or longer, to go from initial planning to implementation.

Proactive planning focuses on the big picture like deciding what tools, services and vendors to have in the arsenal, to deciding what the overall risk architecture or platform will look like and who that primary fraud solution provider will be. These are major strategy changes that require extensive planning and research to understand how it will impact many different areas of the business and profitability.

Proactive planning should also be driven by annual reviews that ensure an organization's fraud prevention strategy and solution partners are still aligned with the business goals and needs, as well as the organization's risk tolerance. It may be that risk tolerance or business goals have changed, or it may be that the strategy needs improvements to realign with these goals and objectives.

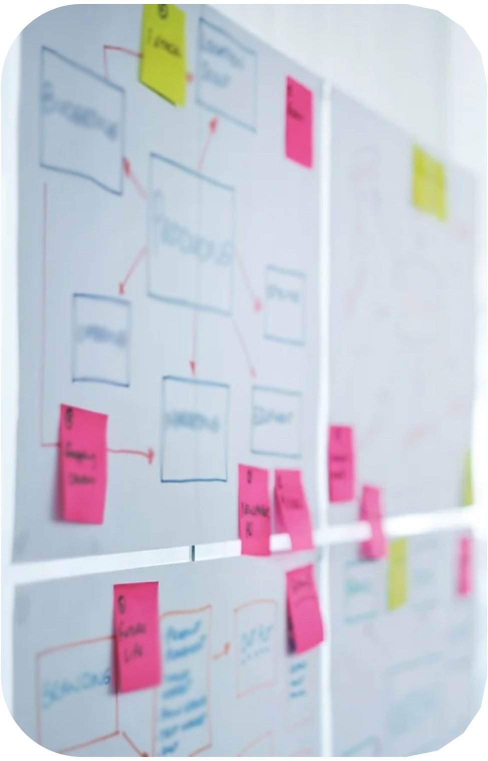
When the quick pivots and incremental changes are not going as far as they used to, considerations around evolving the long-run strategy should already be underway. Proactive planning must consider where the response to new and evolving fraud attacks may be falling short. Define and determine what key features or tools are required to maintain the efficacy of quick pivots and what broad strategy improvements are required to provide these capabilities.

Terms and Definitions:

Tools — the in-house or third-party data sources, applications or technologies used within a fraud solution.

Technique — the methods for applying business processes, policies, experience, logic or modeling to evaluate, predict or determine a potential outcome. May comprise one or multiple *tools* to produce one or multiple derived *signals*.

Signal — the data elements, actual or derived, that are used within the risk architecture or platform to influence a fraud or risk related decision.



There are many examples of this over time, and there will be many more to come as fraud prevention technology evolves. Historically, this has included the decision to evolve from a rules-based to model-based risk architecture. This also includes adding tools and new signals to the existing architecture, such as adding behavioral signals as variables to leverage within fraud coring models. Proactive strategy planning includes considering what new risk signals are needed, how they will be leveraged and what vendors should be considered to provide them. Beyond the availability of data and risk signals, organizations should consider the accuracy of the data, as this data feeds the fraud prevention platform and impacts the ability to accurately detect fraud.

Considerations within this strategic planning also include determining what aspects of the strategy are managed in-house—versus what will be accomplished with the help of a solution provider. Different types of organizations will have varying levels of expertise, budget and capabilities that drive these decisions. Consider the ability to support the roles or teams required to manage various aspects of the strategy internally. The personnel and expertise required to manage internal risk models with data scientists is very different from what is required to make minor adjustments with a modeling platform that provides initial models and adaptive machine learning, or relying completely on a managed service.

“Defending your business and customers against the complex, living Fraud Economy takes a bit of fighting fire with fire. Cybercriminals use AI, automation, and other advanced toolsets to exploit security vulnerabilities at every level, on any channel they access—launching everything from automated scams to synthetic identity attacks, social engineering schemes, and large-scale, brute-force account takeovers—in a matter of seconds. Merchants have to be equally as equipped with intelligent automation and data-backed tools to plan and react to abuse with the same sophistication and speed.”

— Kevin Lee, VP of Trust & Safety at Sift

Comparative Review: Quick Pivots versus Proactive Planning

Quick Pivots	Proactive Planning
Reactionary responses to new ***fraud attacks***	Develop long-term, data-based strategies that keep pace with evolving fraud prevention technologies and emerging ***fraud trends***. *If it's not proactive, it's too late!*
Frequent, incremental changes – lots of small and (relatively) easy improvements that add up	Infrequent, major changes that are more difficult to implement but make significant improvements
Rapid implementation – day, weeks, at most months	Long cycle – Several quarters, if not 1 year or longer, from planning through implementation
Leverages the existing tools, technologies and platform	Enhances or replaces current tools, technologies and platform
Depends on **Proactive Planning** to ensure that the tools and platform are sufficient	Relies on **Quick Pivots** for making continual adjustments that ensure optimal use of the platform and technologies
Without **Proactive Planning**, operational abilities for implementing Quick Pivots rely on legacy systems that eventually become obsolete	Without **Quick Pivots**, the long-run strategy becomes stale and fails to maintain or perform at full potential

Evaluating Solution Partners with a Focus on Quick Pivots

When it is time for an organization to respond to a fraud attack and implement quick pivots, they are beholden to the tools and capabilities currently available to them, a reality dictated by the organization's upkeep and proactive planning. Although evaluating current and prospective fraud solution providers is within the scope of proactive planning, any current or potential limitations that hinder an organization's ability to implement quick pivots is a critical consideration that drives these major strategy decisions.

Discussions around evaluating solution partners applies to both a review of current solution providers as well as considerations around evaluating prospective fraud solution providers, whether that is additive to the current strategy or displaces the incumbent platform. It may be part of an annual review to ensure the current fraud prevention strategy and capabilities still align with the organization's goals, or if long-term strategic planning was not as proactive as it should have been, this review may occur mid-year in response to a fraud attack that was not effectively contained. In either case, consider the solution provider's role in helping accomplish the tasks required to pivot or respond to a new payment fraud attack.

Although adding or replacing a fraud solution vendor is part of proactive planning, these decisions directly impact the ability to execute quick pivots.

Businesses considering what they need to maintain effective responses to fraud attacks with quick pivots can refer to the three steps to containing fraud attacks listed previously:

1. **Recognize the attack and it's characteristics**
2. **Determine how to stop it**
3. **Implement the changes required to effectively stop it**

Recognize Different Attacks and Their Characteristics

The first step to correcting a problem is to identify it, and that's where reporting is an essential component of any fraud prevention strategy. Many organizations conduct their reporting in-house, but determining if there are features or alerts from a fraud solution provider can help flag anomalies or supplement internal reporting.

Consider what a potential fraud solution provider can offer both in terms of what risk signals they can help provide for use within reporting and when those signals can be leveraged.

While reporting may primarily be an internal process, it is ultimately signals from payment and fraud solution providers that feed this reporting. Better yet, the fraud solution provider can help identify when something doesn't look quite right. This can range from an increase in declined orders over a short period of time to detecting concentrated activity around certain SKUs, IP ranges or other characteristics associated with an uptick in declined orders.

If an organization fails to recognize an attack until the chargebacks come in, then they are already too late to respond. There should be a focus on detecting spikes in activity as it occurs, as this is the difference between containing a fraud attack versus responding to one after significant damage has already been done. When evaluating vendor solutions, the emphasis should not just be on what signals they can help your organization leverage for reporting, but when those signals are available to guide operational decisions and quick pivots.

Organizations often focus on internal data. This might be data signals available through a fraud solution vendor, but data that is related to the organization's users or transactions. There is tremendous value, however, in also looking outward. An often overlooked aspect is the added value of risk signals derived from cross-merchant data sharing.

Measuring how effective an organization is at detecting and containing fraud attacks is not just the about ability to do so, but how long it takes.

Fraud prevention strategies often focus on containment and stop the second or third fraudulent order attempt based on repeat use of data points, but cross-merchant data sharing allows an organization to benefit from the attacks or losses already experienced by others. This can include recognizing a flagged payment instrument, shipping address or other data point that has been used excessively with other organizations very recently.

Data sharing capabilities effectively eliminate the need for internal reporting to identify and stop the issue. Rather than adding a data point to a negative list, the fraud solution provider already has it on theirs. Steps one through three are effectively taken care of—detection through implementation of the solution to stop the attack happen automatically, as part of the data sharing capability, and demonstrate how shared data signals are leveraged within risk decisioning.

Sift's global data network consists of 34,000+ customer sites and apps worldwide, processing over 1 trillion events per year.

When evaluating fraud solution providers, first consider whether cross-merchant data sharing is supported, then consider breadth of data. In short, the more organizations participating in the data sharing pool, the more likely all participants are to see data points that have been previously implicated by high frequency use or attacks against others.

Determine How to Respond to Fraud Attacks

Outside of data sharing, most reporting that uncovers anomalous or high risk activity requires decisions on how to implement new rules or model features that effectively stop or contain the fraud attack that is unfolding. This ranges from simply adding a data point to a negative list, requiring compound rule or considering a multitude of signals to weigh more heavily within a model-based risk score.

Determining how to stop the current fraud attack begins with knowing what tools and capabilities should be leveraged to contain and stop it. If the most effective way to put an end to the fraud event is outside of the organization's current capabilities, then this becomes a problem that needs to be solved with a longer-term strategy decision.

When evaluating vendors, think critically about the tools and technology that will best support making quick pivots against payment fraud attacks. Determine the security gaps in your current tech stack and identify any tools or platforms that could be contributing to the manual review team's workload.

If the current tools and solutions fail to stop new fraud attacks, this needs to be communicated to the strategy side of the business and lead to a collaborative discussion on what additional tools and signals would reduce the vulnerabilities within the fraud strategy.

Implement the Changes Required to Stop More Types of Fraud

Beyond how an organization's fraud solution providers support the capabilities to stop new fraud attacks with quick pivots, there are considerations around the time, efficiency and operational requirements to put the incremental changes into effect. Once you've determined how to stop a fraud attack, the next task is executing the required steps to put those changes into production.

When evaluating current or prospective fraud solution providers, consider the accessibility and ease of use of their platform or user interface (UI), and how this will enable the organization to implement the quick pivots and iterative improvements as they are needed.

Think about how these tasks are accomplished today and how they could be accomplished in the future. Consider what steps to implementing changes in response to fraud attacks require operational steps, or need a human performing the implementation. This includes tasks like adding or editing rules, adding data to negative lists and providing recent data related to a fraud attack to retrain or update risk models. Determine if there are any features that not just detect fraud attacks, but automatically implement the changes in response.

True machine learning capabilities enable intelligent and real-time refinement of risk models. Similar to the points made around data sharing capabilities, this effectively covers all three steps from detection, to determining how to contain or stop an attack, to the execution of stopping it. However, it's important to consider the timeline here. Understand how quickly models adjust to unfolding attacks, as this could vary between retraining that occurs on set intervals versus refinements that occur variably based on the recognition of new patterns or attacks. Also consider whether fraud losses need to occur to influence when the model retrains, or if smaller iterations and changes to the model or risk weighting can occur in response to spikes in certain activity before that activity manifests as a fraud loss.

There is a tradeoff with the level of control that an organization may want to maintain over models or risk decisions and the level of in-house expertise required to handle this.

Lastly, consider the degree of human capital and expertise that is needed to manage this in-house. Some fraud solution providers supervise models and make incremental changes on behalf of the merchant, whereas some allow machine learning to continue unsupervised and may allow the organization to review model iterations. Further, consider whether a fraud manager or director has access to make changes in the platform or provide specific data for retraining and focusing the models toward making these quick pivots as needed.

Evaluating Solution Partners with a Focus on Proactive Planning

The act of evaluating fraud solution providers is an essential aspect of maintaining a payment fraud prevention strategy that does not grow obsolete. It is critical to maintain a proactive and forward-looking approach to this, as organizations who find they are relying on legacy systems have waited too long and likely now feel rushed to make a decision and migrate to the new platform or provider. A proactive approach is much better than rushing into contractual commitments with a new primary fraud solution provider. This means reviewing what is in place today and determining whether it continues to keep pace with the evolving nature of fraud and the attacks being seen currently.

Organizations should be proactive by reassessing their business needs and risk tolerance, ensuring their current risk strategy still meets these needs.

Although organizations who did not maintain proactive strategy reassessments may find themselves with a need to move on to another primary fraud solution provider, those who reassess more regularly may find that their incumbent provider is still the best option. Annual assessments that ensure your current fraud prevention strategy and capabilities still align with your risk tolerance and business needs is the preferred approach.

Organizations performing this exercise should first focus on what they need from their primary fraud solution architecture or platform. Identify if there are any aspects of being able to respond to new fraud attacks where this platform has been the source of limitations or inability to respond effectively. Determine if a limited ability to respond or implement a quick pivot is a limitation of the primary risk architecture, or due to a lack of tools or risk signals for this infrastructure to leverage.

It can be uncomfortable, but to be thorough an organization must consider not just the platform, tools and risk signals, but how this is all leveraged within the organization. Be fair but also honest in this assessment. **A lousy carpenter blames their tools, but a lack of effective tools will reduce the quality of a skilled carpenter's work.**

If the fraud prevention strategy owner has a track record of strong performance and it is citing a lack of tools or limitations of the platform as the primary issue today, there is a good chance they are correct in that assessment. However, if the organization's fraud prevention strategy owner has limited success despite changing primary solution providers somewhat frequently, there should be a closer look at the common denominator.

The first stage of this proactive strategy assessment is to understand the scope of the change, if one is required. This begins with determining whether additive changes are required, or if the best solution is to completely change the primary fraud solution provider and the platform or risk architecture they provide. The intent of this assessment is not to assign blame, on the solution provider or the fraud prevention director, but rather to identify vulnerabilities and areas of growth.

Additive Strategy Improvements

Some strategy changes are additive in nature. The overall platform or architecture is fine, but it needs more tools and risk signals to leverage in risk decision-making. This is a proactive strategy improvement, but not a major overhaul. These types of changes take closer to months or a quarter to plan, review and implement—as opposed to multiple quarters or years.

Starting with the current fraud solution provider, consider whether they have additional tools that can be easily implemented within their architecture. This could be additive technology or identity tools, for example. Start with the a-la-carte tools they may offer and determine if you have access to all of the relevant tools and risk signals. These may be provided by the fraud solution platform directly, or via an industry partner. If a-la-carte point tools are offered with direct integration, these are typically easy to implement with the "flip of a switch."

The ability to incorporate internal or third-party data signals within the primary fraud prevention platform is a critical consideration when selecting a fraud solution provider.

Leveraging internal data points or signals from a third-party point tool that is not partnered or integrated with the primary platform can be more of a challenge. First consider if it is possible to consider these signals within the primary risk architecture, then the ease or difficulty of integrating it. If the current platform cannot support or make use of these new tools and risk signals, then additive improvements are a moot point. This more than likely means a wholesale strategy change is required.

For organizations actively evaluating new platforms or primary vendors, consider the flexibility for added risk signals down the road. The flexibility to make these improvements by leveraging an organization's internal data as a custom data field, or other third-party tools or signals, is a valuable feature that can increase the longevity of using the primary vendor's platform.

Beyond the ability to respond effectively, consider the flexibility and speed to respond to new fraud attacks. If speed or flexibility is the issue, then it is less likely that an additive strategy improvement will fully address the problem. It is more likely that the organization will need to replace their primary fraud solution provider or legacy internal architecture.

Since switching primary fraud solution providers is such an extensive effort, it is much better to do this proactively rather than as a rushed and reactionary response.

Wholesale Strategy Changes

Migrating from one primary fraud solution provider to another is a major undertaking that requires extensive effort around technical integration, testing, refining and gradually flowing more activity from the previous to the new primary solution provider. Organizations are often reluctant to make these changes, and often only do so when there is an evident need. Unfortunately, the evident need to make the switch is a problem in itself, as that means fraud losses, sales conversion or operational efficiency are suffering – if not all three. It also means the strategy revisions were not proactive enough.

Although it may be painful to admit it, sometimes wholesale strategy changes are required, such as when an organization is reliant on a legacy system or architecture, whether internal or provided by a third-party vendor. Although such a change is a high-level strategy decision, it is important to consider how these changes will benefit your fraud teams day-to-day and measure the potential success not just on the ability to prevent fraud, but the ability to enable more sales and reduce operational costs, such as around manual review.

Beyond reducing fraud, a wholesale strategy change is typically also justified with improvements in terms of sales conversion and operational efficiency.

Switching to a new primary fraud solution provider is a major decision that needs to be examined from many perspectives. Consider how the new platform will improve capabilities to react with quick pivots, and work with the operational leads of the fraud team to ensure this new strategy will provide the capabilities and tools they need. This could include making lists of features that are must-have versus nice-to-have.

Another useful approach is to start by considering the problems that persist today. Consider how a new fraud solution provider would address the gaps that couldn’t be addressed with the incumbent provider or homegrown platform. This might be related to the ability to detect fraud attacks as they occur via reporting, having the right tools available to derive meaningful risk signals or the ability to promptly implement changes when needed.

Beyond considering the tools and risk signals that a primary fraud solution provider can support, ensure the risk decision-making platform can effectively leverage these signals. Managing risk is fundamentally about making decisions in the face of uncertainty. While more signals can reduce uncertainty, both the quality of those signals and the ability to turn those signals into a decision impact the overall performance of the risk management strategy.

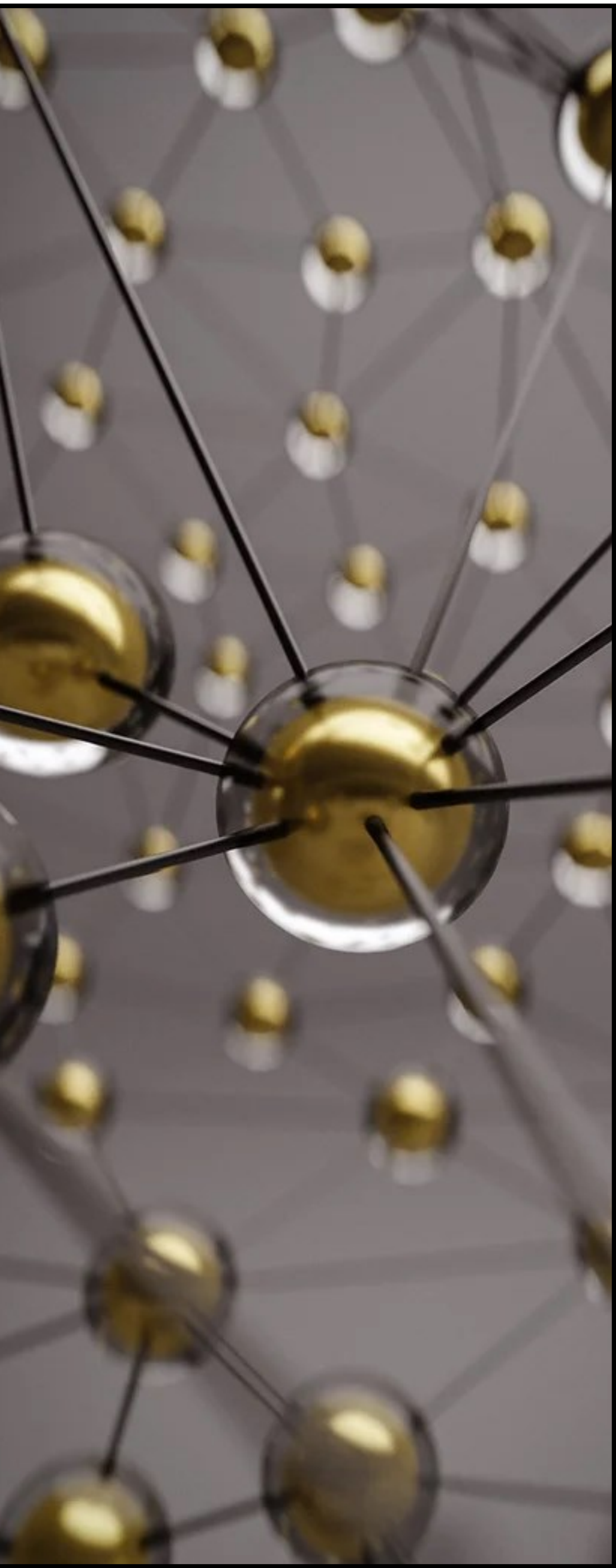
Taking a truly proactive approach considers not just what is needed today, but what will be needed in the future. Organizations have different preferences in terms of the level of transparency, ranging from just wanting a numerical risk score to having an explanation of how that score was determined. There is also a range of preferences and a tradeoff around an organization's level of control. If an organization wants to have more control over when and how to retrain models or modify score thresholds, they need the in-house expertise and assets to drive good decisions when making these changes. These preferences tend to be more static over time. Other needs are more likely to change, particularly around scalability and automation for merchants in high-growth stages.

If an organization feels the need to move on from an incumbent vendor or internal platform, it is likely that they failed to keep pace with fraud and evolve overtime to the business needs. Often organizations find that they have outgrown their current payment fraud prevention platform as their volumes, risk profile or risk tolerance has changed. Beyond considering what the organization needs today and how that differs from what the incumbent vendor offers, consider how business needs will likely continue to evolve into the future.

With respect to leveraging risk signals in decision making, consider not just the availability of signals, but also the quality of these signals and how quickly they can be acted upon.

If a fraud solution provider proactively improves their technology, platform and capabilities, this can alleviate much of the strategy work for the merchant or organization. Consider this when choosing a new solution partner. Is this a solution provider that will ultimately need to be replaced in two-to-five years, or are they evolving their service offering as fraud continues to evolve in both methods and sophistication? Organizations won't have to replace a legacy system if the fraud solution provider prevents their platform from becoming a legacy product. At worst, the solution provider will migrate their clients from one system to another as they evolve or replace their platform.

Whether an organization has to initiate this change by switching fraud solution providers, or whether the solution provider evolves to maintain their clients, the key is that this is done before the current solution becomes a legacy platform.



Conclusion

Effective fraud prevention strategies do not stay effective indefinitely, they are maintained. Their effectiveness requires the ability to execute quick pivots in response to an infinite number of possible fraud attack characteristics, while maintaining a long view on the proactive overhauls and major strategy changes that will one day be required – with an emphasis on making these changes before the overall strategy deteriorates.

While proactive planning and quick pivots are often discussed as different components and methods for maintaining an effective fraud strategy, it is important to consider how these approaches are intertwined. Quick pivots respond to what cannot be foreseen, maximize the effectiveness of the primary fraud prevention platform and continue to improve the performance of the overall fraud strategy. A proactive strategy approach is required to enable quick pivots to be effective and ensure new tools, if not a new risk architecture, are there to support day-to-day payment fraud prevention operations.

Proactive planning should consider what tools, services and techniques organizations should have in their toolbox, and should be reevaluated with annual reviews to ensure continued alignment with business goals and objectives. Sometimes the organization’s goals and objectives change, and sometimes the fraud prevention strategy can no longer perform at a level that meets these objectives.

Evaluating current and prospective fraud solution providers is an essential aspect of maintaining a payment fraud prevention strategy that does not grow obsolete, while what it takes to fight this obsolescence ranges from making additive changes to a complete strategy overhaul.

Ensuring a fraud prevention strategy has the tools and capabilities to quickly respond to and contain fraud attacks is essential. The continued ability to make such pivots and incremental changes is contingent on long-run strategy planning and a proactive approach to ensure that the payment fraud prevention strategy continues to evolve and keep pace with both the speed of industry innovation and the sophistication of professional fraud attacks.

Fraudsters will seek out the path of least resistance, which means they will move away from targets with robust and current fraud prevention strategies while seeking out low hanging fruit. As a result, organizations that do not evolve their risk management strategies alongside industry innovations are likely to find themselves the new target of sophisticated fraudsters and fraud rings. Not only will this result in large fraud losses, but it will likely have detrimental impacts in terms of sales conversion and inflate operational costs.

For organizations with a meaningful user base or sales volume, it’s not a matter of ***if***, but ***when*** they will see these payment fraud attacks. The question is whether they are still equipped to prevent it.

About the Fraud Practice

The Fraud Practice is a privately held company based in Palm Harbor, Florida. The Fraud Practice provides training, research, and consulting services on eCommerce payments, fraud prevention, and credit granting. Businesses throughout the world rely on The Fraud Practice to help them build and manage their fraud and risk prevention strategies.

For more information about The Fraud Practice's consulting services, please visit www.fraudpractice.com. For additional information about The Fraud Practice's online training programs, please visit www.CNPtraining.com.

The Fraud Practice
www.fraudpractice.com
www.CNPtraining.com
Telephone: 1.941.244.5361
Email: Questions@fraudpractice.com

Are you looking for answers or solutions, for eCommerce payments and fraud management? Give us a call for a free introductory consultation to see if we can help you. Even if we can't meet your needs we most likely know someone who can, and we are happy to provide you with contacts of reputable firms and individuals servicing the space.

David Montague,
Founder

About Sift

Sift is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of one trillion (1T) events per year, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Twitter, and Wayfair rely on Sift to gain a competitive advantage in their markets. Visit us at sift.com and follow us on LinkedIn.

THEFRAUDPRACTICE
PROTECTING THE BOTTOMLINE

connect to address 192.168.1.10
username: *********
password: ***********
Access granted...
exited after 0.006146 seconds with return value
any key to continue . . .

PAYMENT FRAUD PREVENTION:

QUICK PIVOTS AND PROACTIVE PLANNING

White paper by The Fraud Practice
Sponsored by Sift