STRATEGIC GROWTH INVESTMENT:

A CFO'S GUIDE to Fraud Prevention, Value Creation, and Risk Management

sift | CFO DIVE

Custom content for Sift by studioID

> **Nearly 90% of businesses saw up to 9% of revenue lost to fraud.**
>
> Veriff US Fraud Industry Pulse Survey

CFOs at high-growth companies have numerous strategic priorities, including AI integration, cash efficiency and working capital optimization, talent management, and business process improvement. Simultaneously, fraud has evolved from a peripheral risk management issue to a central concern for the finance department. A Veriff U.S. fraud industry pulse survey found that nearly 90% of businesses saw up to 9% of revenue lost to fraud, which could significantly undermine profitability efforts.

While fraud prevention and operational risk can fall under the purview of the finance department, they often reside in various departments, including cybersecurity, operations, compliance, customer service, IT, and legal. For many, fraud represents a significant source of financial loss that directly affects profitability, revenue streams, and long-term growth. Businesses now face an expanding range of risks driven by sophisticated emerging patterns, and newer techniques for orchestrating payment fraud have become a ubiquitous problem for enterprises. Case in point: today, payment fraud represents more than 3% of all attempted transactions across the Sift Global Network. But at the same time, fraud prevention also creates a number of avenues for materially fostering growth and improving the customer experience.

This playbook offers CFOs a comprehensive framework for understanding, quantifying, and mitigating the economic implications of fraud. Traditional fraud metrics often underestimate the true organizational cost. CFOs should now consider risk-adjusted financial models to best manage the changing fraud landscape. This guide goes beyond the typical 5-9% loss estimates, revealing how fraud undermines financial performance. It also illustrates how fraud prevention can be a force multiplier for customer experience and a lever for profitable growth.

Executive Summary

Leading CFOs now recognize fraud prevention as a profit center, not just a cost center. It is now a strategic function that delivers measurable ROI through better approval rates and reduced friction at every stage of the customer journey, resulting in lower overall customer acquisition costs. Nonetheless, increasingly sophisticated fraud attacks continue to stretch the capabilities of many fraud departments, making the ongoing investment in the latest solutions critical.

As a result of this shift, today's CFO has an expanding role in fraud leadership. They now own the direct losses, operational costs, compliance-related costs, and expenses associated with declined yet legitimate customers and transactions. CFOs have shifted from a peripheral role in fraud technology decisions to becoming the primary buyers of fraud solutions. As such, there's now demand for ROI guarantees and performance-based service level agreements.

There's also a pronounced shift in customer expectations. According to Veriff, over 86% of U.S. fraud decision-makers say their customers are now more demanding regarding robust fraud prevention capabilities.[1] And with good reason. The Federal Trade Commission recently announced that consumers reported losing $12.5 billion to fraud in 2025, a 25% increase over the previous year.[2]

From a strategic perspective, ineffective fraud operations increase costs, put brand reputation at risk, and, in some cases, expose the business to regulatory risk. Consequently, companies that invest and optimize their fraud programs achieve significantly better financial performance than those with less refined approaches.

Ways to Reframe Fraud as a Growth Engine

Reassess Fraud's Full Business Impact

- Go beyond direct fraud loss numbers.
- Quantify the impact on **customer churn, customer lifetime value (CLTV), manual review overhead, and false positives** that block good customers.

Link Fraud to Revenue Leaks and Operational Inefficiencies

- Identify areas where outdated or rigid fraud systems are causing **revenue leakage**—such as checkout abandonment, unnecessary declines, or friction-filled account creation processes.
- Calculate the hidden costs of manual processes and operational inefficiencies.

The Business Case for Strategic *Fraud Prevention* Investment

Financial Impact

The true cost of fraud extends far beyond direct losses, creating a cascade of financial impacts. Beyond the up to 9% revenue leakage, additional impacts make mitigating fraud losses critical for enterprises. In the face of fraud, a brand's reputation and customer trust metrics often suffer. Fraud can also significantly affect customer lifetime value preservation as it often results in customers spending less or severing their relationship altogether.

Fraud also comes with operational costs that extend beyond the fraud department to impact every department that must interact with and assist a customer in the aftermath of fraud. Consequently, organizations that minimize fraud and its impact can capture significant and sustained operational efficiency gains.

Growth Opportunities

Fraud prevention is at the heart of every superior customer experience. Managing friction involves accelerating the approval of legitimate customers and transactions, minimizing operational inefficiencies, and optimizing the user experience to support long-term customer value while mitigating fraud risk.

In crowded marketplaces, superior fraud controls can serve as a competitive differentiator. This includes accepting legitimate customers that a competitor would decline, operating in markets that others are ill-equipped to serve, and processing transactions faster and with confidence, undoubtedly improving customer satisfaction.

With a strong foundation, there's potential to scale the approach to fraud prevention and expand into new or existing markets with confidence.

According to McKinsey, when customers experience fraud, it hurts the customers' trust and their willingness to use services. McKinsey also found that of banking customers who were fraud victims, 70% reported higher levels of anxiousness, stress, displeasure, or frustration when notified of potential fraud. However, when companies respond well to actual fraud, McKinsey found that customers reported higher levels of satisfaction as well.[3]

Ways to Reframe Fraud as a Growth Engine

Collaborate with GTM Teams to Align on Growth Metrics

- Partner with Product, Marketing, and Sales to align fraud strategy with **customer experience, conversion rates, and expansion opportunities.**
- Shift fraud metrics from loss avoidance to **growth-enabling KPIs** (e.g., approval rates, good user pass-through rates).

Invest in Adaptive, AI-Driven Fraud Platforms

- Replace legacy rules-based systems with AI-powered platforms that **learn and adapt** in real time.
- Choose solutions that improve accuracy while **minimizing friction for good users,** unlocking faster growth and greater scale.

Reframe the ROI of Fraud Technology

- Build a business case that includes **prevented losses, operational cost savings, improved customer retention, and conversion uplifts.**
- Emphasize the platform's role in **unlocking new markets, accelerating account growth, or supporting new product launches.**

Economic *Impact* Analysis

Cost Structure

Establishing and optimizing the cost structure of a fraud solution requires focusing on three elements. First, direct losses and acceptable loss thresholds based on benchmarks and tolerance. This requires establishing loss metrics based on industry benchmarks and the organization's tolerance for risk. It also requires a granular approach that defines fraud rates by transaction type, customer, product, and geography.

Second, businesses must pay attention to operational costs. It's critical to calculate total fraud prevention expenses, including direct expenses such as software, staffing, and infrastructure, and indirect costs, including customer service.

Third, recovery and remediation expenses such as investigation costs, legal fees, compliance-related fines and penalties, and customer reimbursements generate significant costs. It should include the effort and expense associated with dispute resolution, case preparation, and any contact with third parties, such as other institutions or law enforcement.

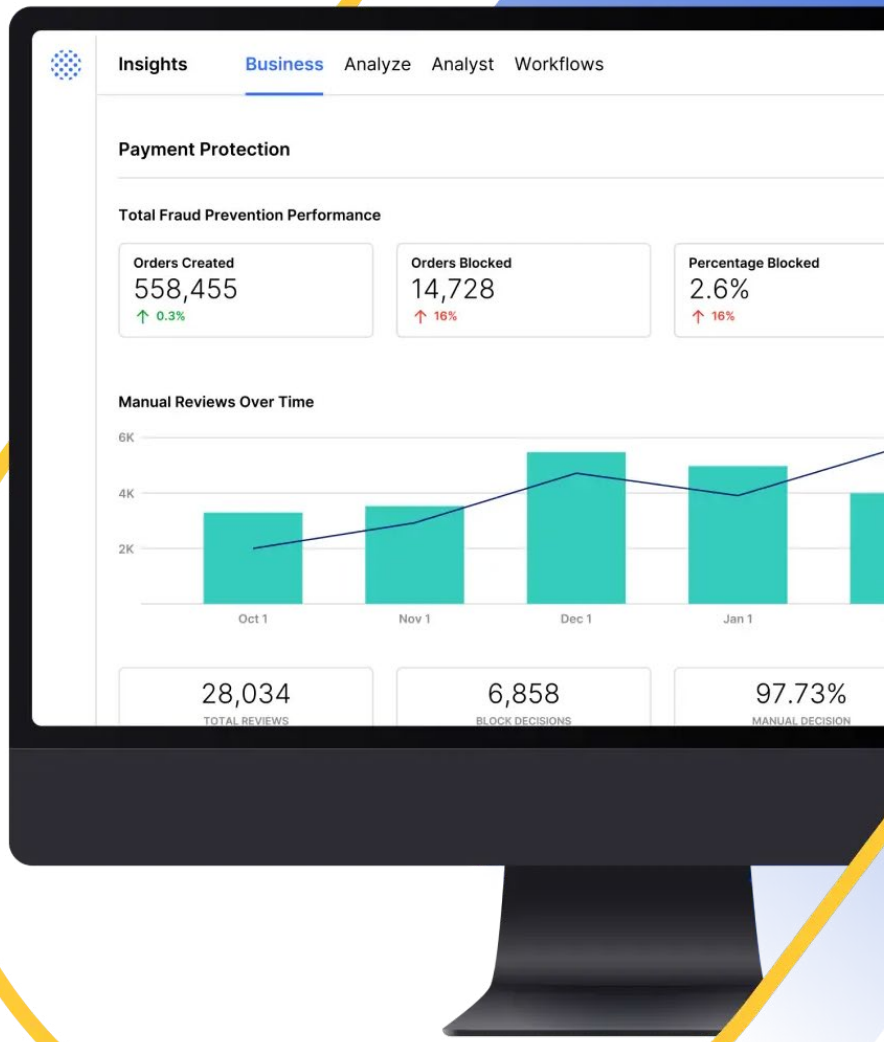
Beyond direct losses, fraud can result in higher payment processing fees, insurance premiums, and additional compliance-related costs, such as extra personnel to manage regulatory reporting. Furthermore, companies that exceed acceptable thresholds set by card networks risk being banned from those networks entirely. Just as importantly, the lifetime value of a customer who experiences fraud, excessive friction, or false declines drops precipitously.

Strategic *Implementation*

Technology Evaluation

When evaluating fraud prevention platforms, finance leaders should prioritize solutions that address the total cost of fraud, not just direct losses. The ideal platform minimizes false positives and reduces the burden of manual reviews. Additionally, vendors should demonstrate their effectiveness through industry-specific benchmarking and concrete proof points relevant to your sector, as fraud patterns and prevention strategies can vary significantly by industry.

The platform's technical capabilities and business impact are equally important. Solutions that offer flexibility and scalability while maintaining low integration and minimal ongoing management requirements allow fraud teams to focus on strategic initiatives rather than system maintenance. Robust reporting and analytics capabilities should provide actionable insights tailored for finance leadership, enabling data-driven decision-making. Finally, the vendor should possess a proven track record of delivering measurable business outcomes for finance teams.



Payment Protection

Total Fraud Prevention Performance

Orders Created	Orders Blocked	Percentage Blocked
558,455 ↑ 0.3%	14,728 ↑ 16%	2.6% ↑ 16%

Manual Reviews Over Time

28,034	6,858	97.73%
TOTAL REVIEWS	BLOCK DECISIONS	MANUAL DECISION

In particular, AI-powered solutions allow organizations to create streamlined customer experiences that increase lifetime value and revenue by minimizing false positives. Effective fraud prevention helps organizations avoid significant financial and reputational damage. This frees up resources to fuel growth investments rather than funding investments to fund damage control. Finance leaders who prioritize AI-powered systems that offer quick time-to-value, seamless integration, and scalability will create competitive advantages, driving predictable growth and customer loyalty.

Ways to Reframe Fraud as a Growth Engine

Socialize Success Stories Internally

- Share tangible examples (e.g., "reduced chargebacks by X%, increased approval rates by Y%, shortened onboarding time by Z%") with internal stakeholders.
- Make fraud wins visible to the board and other C-suite leaders.

Build Fraud Strategy into the Broader Digital Transformation Agenda

- Position fraud technology as part of a broader effort around **automation, digital trust, and customer-centric growth.**
- Advocate for fraud strategy inclusion in enterprise-wide initiatives like CX transformation or data-driven decision-making.

Risk Management and *Security* Measures

Threat Prevention

Of the threats facing organizations, payment fraud and account takeover (ATO) are the most significant and potentially damaging. AI sits at the center of these attacks. According to research conducted by Veriff, nearly 78% of U.S. decision-makers observed an increase in the use of AI in fraudulent attacks over the past year.[4] In a recent press release, Visa warned of a surge in application fraud in digital banking powered by artificial intelligence. This includes a 244% year-over-year increase in digital document forgeries. Furthermore, deepfakes accounted for a staggering 40% of biometric fraud attempts.[5]

Nearly 78% of U.S. decision-makers observed an increase in the use of AI in fraudulent attacks.

Veriff US Fraud Industry Research

When an account is taken over, businesses face direct losses from unauthorized transactions, potential chargebacks when the bad actor compromises the customer's card information on file, and the loss of customers who close or abandon their accounts. Many organizations struggle to measure the downstream effects, such as lost customer lifetime value and acquisition costs, as they fall outside of routine fraud metrics.

However, data does exist to help fraud departments optimize their approach. Sift reported an account takeover attack rate of 3.2%, with a 12% two-factor authentication rate for all industries. Not surprisingly, the rates vary significantly by industry. The ATO attack rate for digital commerce increases to 3.8%, and the two-factor rate drops to 9.8%. The ATO attack rate for finance and fintech is 1.7%, with a two-factor authentication rate of 17%.[6]

Synthetic fraud is often called the "long con," as it takes time for bad actors to build accounts with sufficient activity to use as part of their scheme. Since synthetic identities appear to all intents and purposes as regular accounts, often the first indication that an account is synthetic appears when fraud happens, and it is impossible to find a victim.

Mobile platforms can create friction and impact conversion and the realization of revenue. Operating systems can limit the data organizations can access in the name of fraud detection, which forces businesses to decide on transactions and accounts with incomplete information. Consequently, there must be a balance between false positives that alienate legitimate customers and the potential for fraud due to incomplete data when a transaction involves a mobile platform.

3.2%

Account takeover attack rate

12%

Two-factor authentication rate

FIBR
powered by sift

How does your digital risk strategy stack up?

Compare your own data against Sift benchmarks with FIBR, the first Fraud Industry Benchmarking Resource of its kind delivering crucial fraud insights to businesses across verticals and regions.

Customer Experience

Finding the balance between keeping bad actors out and not alienating customers is a perplexing problem for many organizations. Generally, high-performing solutions only add friction when it is critical to decisioning a transaction or account. There's also a role for behavioral analytics that analyzes customer activity in parallel, therefore exerting minimal, if any, additional friction.

Too much security increases the likelihood of abandonment, incomplete registrations, and losing customers to competitors, whereas a false positive may alienate a customer permanently.

There are also industry-specific considerations. In financial services, customers are generally more tolerant of friction than in customer-facing marketplaces. This makes invisible or minimally invasive security measures more critical for specific industries.

The Bottom Line

Fraud creates many indirect and direct impacts within an organization. Successful fraud prevention requires removing siloes between the departments that play a direct and indirect role in loss mitigation and management. AI-powered fraud prevention counters these effects by minimizing losses, improving customer retention, and reducing friction.

Sift is the AI-powered fraud platform deliverying identity trust for leading global businesses. Our deep investments in machine learning and user identity, a data network scoring 1 trillion events per year, and a commitment to long-term customer success empower more than 700 customers to grow fearlessly. Brands including DoorDash, Yelp, and Poshmark rely on Sift to unlock growth and deliver seamless consumer experiences.

Visit us at sift.com and follow us on LinkedIn.

Sources

1 https://www.veriff.com/resources/ebooks/veriff-us-fraud-industry-pulse-survey-2024

2 https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

3 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience

4 https://www.veriff.com/resources/ebooks/veriff-us-fraud-industry-pulse-survey-2024

5 https://fintechmagazine.com/articles/visa-warns-of-application-fraud-surge-in-digital-banking?

6 https://sift.com/fibr-fraud-industry-benchmarking-resource/

studio / ID BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more