DIGITAL TRUST & SAFETY

The Next Big Thing for Luxury E-commerce Fraud Management

VISEO DIGITAL MAKERS

sift

Rachel Buillet
E-Commerce & Fraud
Consultant VISEO USA

Michelle Arguelles
Sr. Product Marketing
Manager SIFT

Tackling Fraud Amidst Changes in Luxury Retail & Buying Behavior

As the luxury retail experience increasingly shifts from brick-and-mortar stores to online channels, retailers are faced with new fraud challenges that are constantly growing and evolving. While buying behavior is changing, customer expectations have not. Luxury buyers expect the same premium, individualized experiences they would get in-store. This requires a proactive and agile approach to tackling fraud. Traditional rules-based systems lack flexibility and adaptability, making it critical to adopt a machine learning-powered Digital Trust & Safety approach that aligns effective loss prevention with premium customer experiences and revenue growth.

Omnichannel and other digital strategies that bridge the gap between e-commerce and in-person sales open brands up to more risk as fraudsters gain a new, easier channel to exploit through card not present transactions. Online sales of luxury goods are projected to triple to $76 billion by 2025, with US credit card losses due to fraud expected to reach $12 billion by the end of 2020, costing retailers, on average, 5.4% of their annual revenue.

In order to stay ahead of the rapidly changing landscape of luxury e-commerce, it is crucial to adopt fraud-fighting technologies and strategies that incorporate a Digital Trust & Safety mindset. In the coming pages, we'll look at some of the common challenges faced by luxury brands when fighting fraud Safety mindset. In the coming pages, we'll look at some of the common challenges faced by luxury brands when fighting fraud and how machine learning can overcome them.

Why do fraudsters target luxury?

When fraudsters hack a PayPal account or gain access to stolen credit card information, they want to maximize their spend as quickly as possible. High-dollar luxury items are a great way to do so. Whether trendy or timeless pieces, luxury items are in high demand (think limited edition sneakers), can have high intrinsic value (like jewelry), and usually retain their value.

Because they are so desirable, luxury items are easy to resell online (sometimes at an even higher price), especially on secondary markets such as Privé Porter, The RealReal, or StockX. This yields quick profits and turnover for fraudsters. Take the iconic Hermès Birkin bag, for example, typically priced between $150-250k. Its elusiveness has been attributed to the discrepancy between its demand that continues to supersede supply. According to The New York Times, Privé Port has sold over $60 million of the bags in only five years!

The reward greatly exceeds the risk for fraudsters targeting luxury. Because of this, they are highly motivated to outsmart fraud systems in place and the people managing them behind the scenes. Some fraudsters even put in the effort of getting a suite of fake IDs and social engineering customer support agents for months before placing an order. As fraudsters' methodologies become increasingly sophisticated, the challenges for luxury retailers grow, and meeting them head on is even more important.

Top Fraud Challenges for Luxury Retailers

Chargebacks: A higher cost for luxury

Like all e-commerce merchants, luxury retailers get hit with a mix of fraud (stolen cards used for purchase) and friendly fraud chargebacks (like using a family member's card or one's own card then denying recognition of the purchase). These types of fraud hurt a company's bottom line and add operational load for manual review and chargeback representment.

Compared to other e-commerce businesses, luxury vendors see fewer orders and higher average values. This means that every individual chargeback costs more, and each one also brings a business much closer to the chargeback limits imposed by credit card companies (<1% for most, with the exception of Visa's more stringent limit of 0.9%). As a result, monitoring this rate over time is imperative.

If you compare a luxury brand against a mass market brand, and analyze the ratio of monthly chargebacks received to incoming orders, you see that the number of chargebacks needed to reach this threshold is exponentially lower for the luxury brand. This is because their business models differ drastically, with luxury brands having a much greater average order value (AOV) and lower order volume.

Whether or not you win a dispute, all incoming chargebacks are accounted for in this percentage. This has pushed merchants to do a better job at fighting fraud, with the risk of being added to an ECMP (excessive chargeback monitoring program). This happens when the above limits are surpassed and a merchant receives chargebacks on over 100 orders on one card type in any given month. If self-correction does not happen within four months, merchants face large fines and can eventually even lose their ability to participate in e-commerce sales.

Chargeback Thresholds: Luxury vs. Mass Market Brand

	LUXURY BRAND	MASS MARKET BRAND
Annual Revenues	$500 MILLION	$500 MILLION
Average Order Value (AOV)	$1,000	$50
Yearly / Monthly Orders	500,000 / 41,667	10,000,000 / 833,333
1% Chargeback Rate	5,000 CHARGEBACKS	100,000 CHARGEBACKS
> Monthly Chargeback Threshold	417 CHARGEBACKS	8,333 CHARGEBACKS

TIPS TO MITIGATE CHARGEBACKS

While a great fraud tool can stop many illegitimate orders, some chargebacks—especially non-fraud and friendly fraud—are inevitable. Because true fraud chargebacks must be counted as losses (unless a merchant has paid for a service with a chargeback guarantee), merchants can focus on several ways to prevent other types of chargebacks:

Provide superior customer service

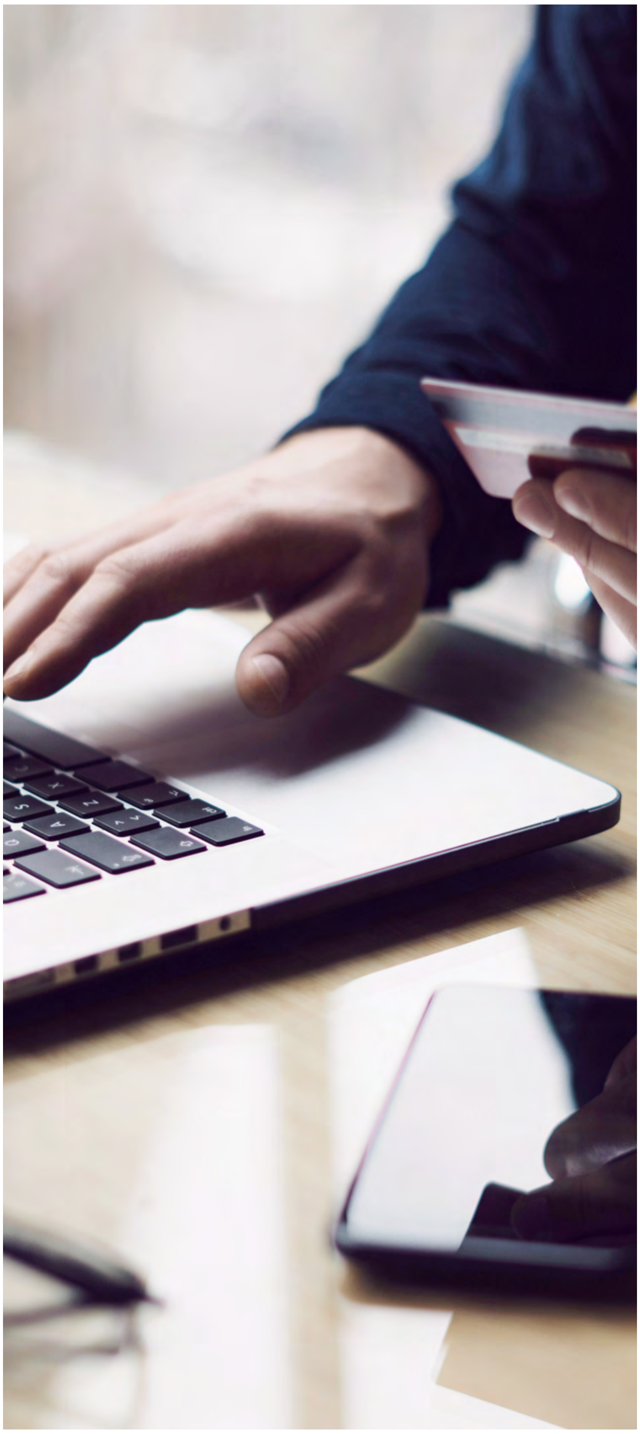
Provide a clear method of contact on your website and respond to messages, calls, and refund requests in a timely manner. Track patterns of dissatisfaction and find ways to solve their root causes. Most non-fraud chargebacks are due to this issue.

Be clear with your product descriptions and policies

Represent products clearly and accurately. Confirm that any return and shipping policies are clearly laid out and easy to find on your website, and that any potential delays are communicated to customers to set the right expectations.

Keep detailed records of all transactions

Make sure that order notes, as well as any customer contact, is clearly recorded, in the event of a chargeback (including proof of delivery with signature).



Look out for chargebacks on refunded transactions

Ensure that the acquiring bank is responding to chargebacks for which a refund was already processed to avoid excessive chargeback counts and additional fees.

Repeat returns: More lost revenue

An increasing number of luxury retailers are banning repeat returners from their websites and including clauses about this behavior in their return policies. These customers are not simply changing their minds. They buy luxury goods (like a trendy new bag or a dress for an event) only to wear once or twice, which they then attempt to return for a refund. If the merchant then refuses to issue a refund, or sends back the returned item, the customer often issues a chargeback, stating the item was "not as described."

In luxury, quality control teams perform stringent checks on the merchandise before it is shipped to the customer, so it is nearly impossible that a worn/damaged item be shipped to a new customer. Operations managers, however, find receipts or gum wrappers in bags customers claim to have never used, or sweat stains on clothing the customer claims were present when they received the item. The merchant is left to consider multiple decisions:

1. Do they accept the return and issue a refund, swallowing the cost of the merchandise?

2. Do they reject the return and risk upsetting a customer and/or getting hit with a chargeback?

3. Do they block the customer from future purchases and risk negative publicity? If so, after how many claims of receiving worn/damaged items?

Repeat offenders of return abuse lead to more loss—both of revenue and of an item that could have been resold.

False declines and excess friction: A hit to top-line revenue

A false decline–also known as false positive or customer insult—is when a legitimate order is blocked in error, often due to inaccurate risk analysis. When this happens, the loss isn't just the single order that was blocked—retailers potentially lose the entire lifetime value of a customer they've turned away. Brand perception is paramount for luxury, so ensuring low false-positive rates is critical for maintaining the positive reputation of the business.

Choosing the Right Fraud Strategy & Tool

Fraud management today is not just about stopping fraud; a complete strategy should also maximize revenue and ensure frictionless experiences for trusted customers. For luxury brands, who feel loss more acutely and whose customers expect only the most seamless experiences, fraud strategies and tools must put the customer first.

There are essentially two types of tools: rules-based and machine learning. While many luxury retailers are still relying on outdated rules-based tools, they are starting to follow other markets in adopting more modern, flexible, machine learning-based tools that are able to adapt to sophisticated fraud patterns in real time, and operate entirely behind the scenes, with as little customer impact as possible.

Rules-based tools and “checkbox” machine learning

As luxury e-commerce and fraud scale in tandem, it is vital for brands to adapt accordingly. Rules-based tools are inaccurate, reactive, and not scalable, and the consequences for the businesses using them are higher fraud rates, lower acceptance rates (processed orders), and higher manual review rates (orders deemed high risk that necessitate human intervention to approve or reject the order). This leads to higher chargeback rates, lower revenue, more false positives, and longer order processing times. Fraud prevention is crucial as it directly impacts top and bottom revenue, and rules-based fraud solutions fall short in the face of growing challenges.

Rules-based systems are limited to analyzing risk uniquely at the point of payment, while machine learning solutions track behaviors along the entire purchase route. They use broad-based criteria to block orders and send them to review. This narrow view often results in missed fraud and with legitimate orders blocked or in manual review. In the following example below, the following rules may be triggered, leading to a high fraud risk score that automatically blocks the order, deeming it as fraudulent:

- Different billing/shipping address
- IP address far from billing address
- Credit card from different country
- Risky item ordered

For example, take an order placed with a European credit card for a Lady Dior handbag that has an IP and shipping address in Los Angeles, but a billing address in New York. This customer may travel frequently for business or have two residences, Yet is being treated like a fraudster. Such a poor customer experience can create a reluctance to return as a customer or negative publicity via social media.

Rules are also reactive, meaning fraud has to happen before it can be blocked. Fraudsters find ways to circumvent the rules in place and may even be able to reverse engineer them, meaning fraud teams are constantly playing catch-up and forced to write additional rules to thwart an adversary one step ahead. This game of cat-and-mouse results in hundreds of rules stacked on top of each other that become impossible to manage at scale.

Many rules-based vendors have seen the shift in the fraud prevention landscape and have added basic levels of machine learning in order to remain competitive. However, at the core of their technology, rules are driving the fraud detection, and their capabilities fall far short of what true machine-learning based solutions can do.

Machine Learning and Digital Trust & Safety: The Future of Fraud Management

As many have discovered the inefficacy of rule-based systems, machine learning-based fraud solutions are penetrating the market. At its core, machine learning refers to the practice of training computers via software to recognize patterns and infer predictions, emulating a human-like ability to learn from "experience." Computers—via specially created algorithms and mathematical formulas—can learn from historical data and suggest likely future scenarios. In the luxury space, machine learning is already widely used to maximize shopping experiences and enhance the sales process. Fraud prevention is a natural, additional use case for this technology.

Machine learning is able to process massive amounts of data, categorize behaviors, unearth patterns, and make connections that humans can't. It is also able to do this across multiple points of the customer journey (e.g. time spent browsing or entering a credit card number at checkout) and proactively detect emerging fraud patterns in real time. Taken together, this results in more accurate predictions, for both trusted and risky orders. It is also very scalable, as a computer is able to sift through orders much faster than a human, leading to more efficient order processing.

After initial setup and training, machine learning tools are almost fully self-automated, and predictions can be used to make instant decisions. This drastically cuts down on the need for human intervention and ensures that merchants are always one step ahead of fraudsters. Machine learning can replace even the most complex rules set and produces higher accuracy, fewer false positives, a lower chargeback rate, and savings through automation.

The right machine learning solution can help you build a Digital Trust & Safety approach, a fraud-fighting plan that aligns risk and revenue decisions. It is more than simply adding a new tool or procedural step—it's about remodeling business strategies for the challenges and opportunities of the digital world.

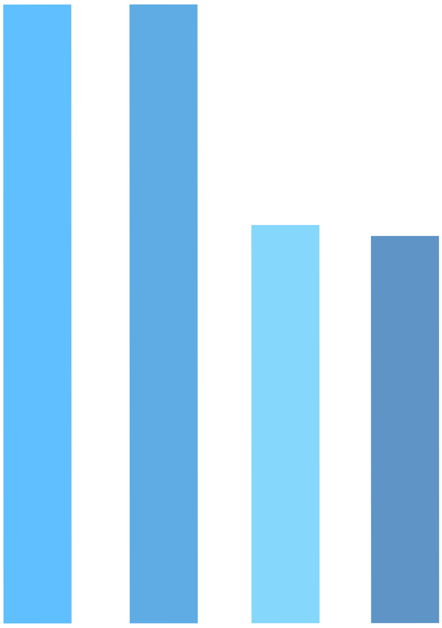
Legacy rules fall short

60% of companies using rules for fraud prevention say rules **BLOCK** legitimate customers

45% say rules **DO NOT** prevent fraud effectively

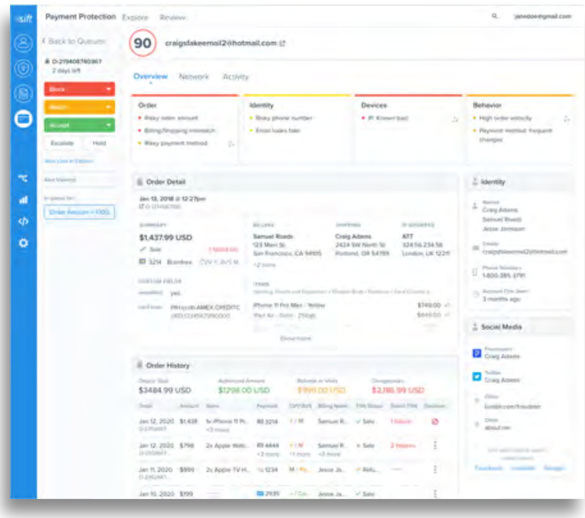
60% say rules **DO NOT** allow them to deliver a frictionless experience

44% say rules **ARE NOT** efficient for the team



Source: Sift Digital Trust & Safety Survey, 2019

Sift: VISEO’s Trusted Partner for Fraud Prevention

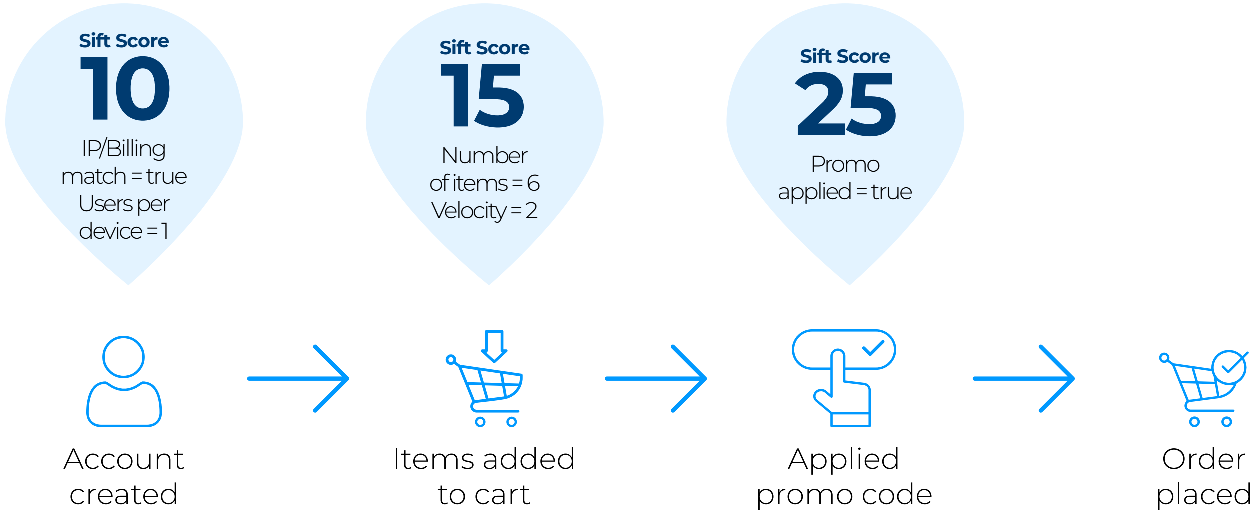


Sift is the leader in Digital Trust & Safety, empowering companies of all sizes to unlock revenue without risk. Sift prevents fraud with industry-leading technology and expertise, an unrivaled global data network, and a commitment to building long-term partnerships with our customers.

Sift uses machine learning to accurately separate suspicious behaviors from legitimate ones. Their unique, real-time approach enables luxury brands to deliver great experiences to trusted customers and stop fraudsters before they can place their orders. Sift customers have seen results like 80% reduction in chargebacks and an average manual review rate of 2.79% (with projected industry averages ranging from 10-26%).

How Sift’s machine learning works

Sift’s machine learning models surface new risks, patterns, and changes in fraudulent behaviors in real time by assessing multiple signals throughout the user journey and global data network, developing a composite score on a scale from 1-100. On this scale, a score of 1 suggests a high level of trustworthiness for a customer interaction, and 100 indicates a high likelihood of fraud; middle-of-the-road scores are surfaced for manual review. This score becomes exponentially more accurate over time.



Sift Score 10
IP/Billing match = true
Users per device = 1

Sift Score 15
Number of items = 6
Velocity = 2

Sift Score 25
Promo applied = true

Account created → Items added to cart → Applied promo code → Order placed

Real-time machine learning

Sift has the unique ability to analyze user behavior throughout their journey, and make proactive decisions that stop fraud before it happens. Its accuracy also allows for frictionless user experiences like one-click checkout for repeat customers.

Global data network

Shared fraud learnings from Sift's network of 12,000 sites and apps around the world offer protection from day one and ensure emerging patterns are caught.

Custom modeling

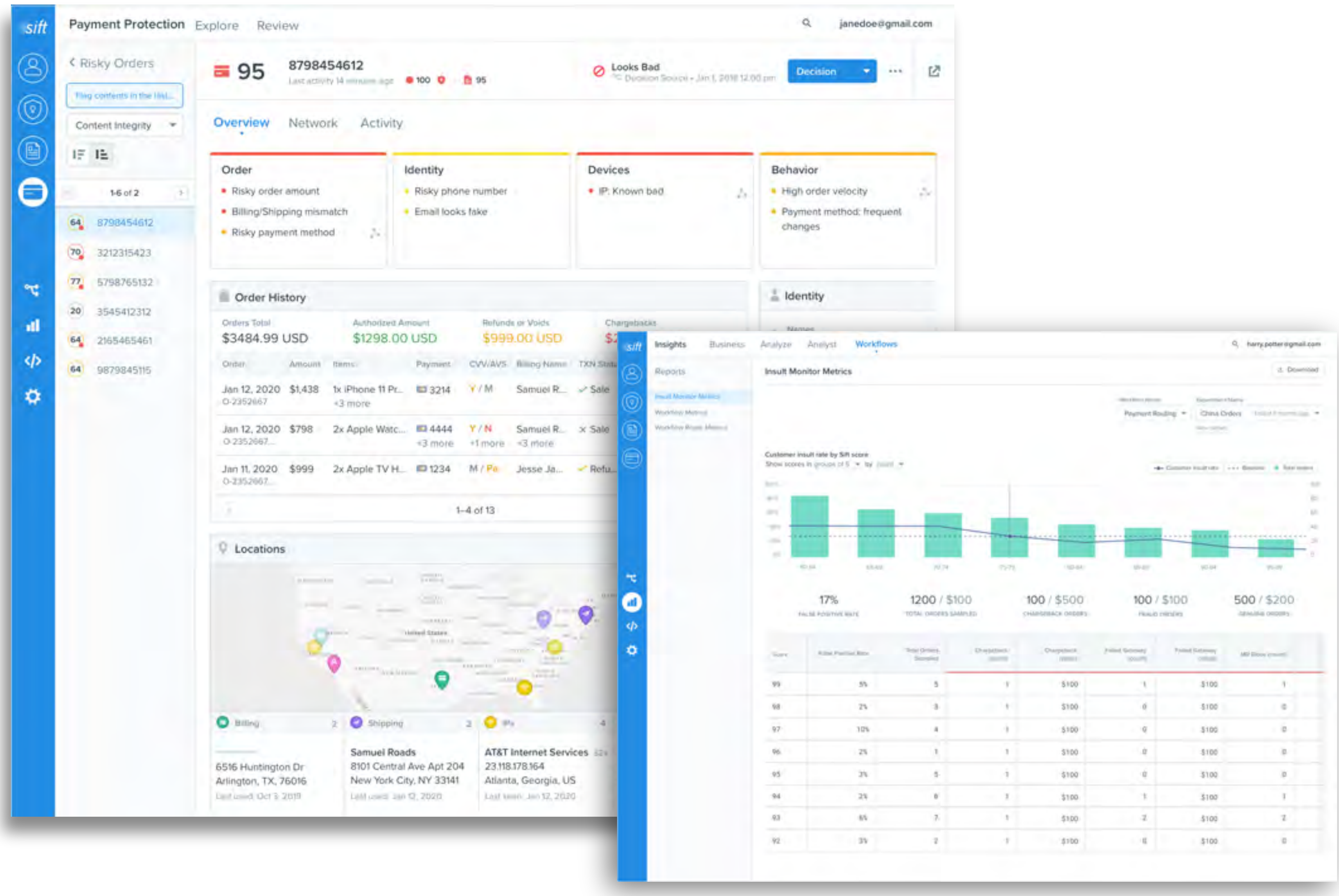
Sift works with each merchant to understand their specific fraud patterns, user behavior, and business needs. From there, we build a tailored machine learning model built to catch a merchant's fraud with unparalleled accuracy.

Automation platform

With Sift, customers can easily automate more—or all—decisions, streamlining operations and reducing manual review efforts that take up valuable human resources.

Analyst Console

The Sift Console provides a visual interface for deep dive investigation and reporting on key KPIs to track fraud performance.



Orders Total	Authorized Amount	Refunds or Voids	Chargebacks
$3484.99 USD	$1298.00 USD	$999.00 USD	$2

Order	Amount	Items	Payment	CVV/AVS	Billing Name	TXN Statu
Jan 12, 2020 O-2352667	$1,438	1x iPhone 11 Pr... +3 more	3214	Y / M	Samuel R...	✓ Sale
Jan 12, 2020 O-2352667...	$798	2x Apple Watc...	4444 +3 more	Y / N +1 more	Samuel R... +3 more	× Sale
Jan 11, 2020 O-2352667...	$999	2x Apple TV H...	1234	M / Pa	Jesse Ja...	✓ Refu...

1–4 of 13

6516 Huntington Dr
Arlington, TX, 76016
Last used: Oct 3, 2019

Samuel Roads
8101 Central Ave Apt 204
New York City, NY 33141
Last used: Jan 12, 2020

AT&T Internet Services
23.118.178.164
Atlanta, Georgia, US
Last seen: Jan 12, 2020

Score	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
99	5%	5	1	$100	1	$100	1
98	2%	3	1	$100	0	$100	0
97	10%	4	1	$100	0	$100	0
96	2%	1	1	$100	0	$100	0
95	3%	5	1	$100	0	$100	0
94	2%	8	1	$100	1	$100	1
93	6%	7	1	$100	2	$100	2
92	3%	2	1	$100	0	$100	0

About VISEO

VISEO is a global IT consulting firm specialized in assisting its clients with their IT and digital transformation. VISEO uses technology as a powerful lever of transformation and innovation to help its clients take advantage of digital opportunities, address new usages and compete with new players who change the rules of the game.

With 2200 employees working on 5 continents, VISEO combines agility and complementarity of its areas of expertise – design of new products and services, digitization of business processes, data valuation, digital assets development - to make digital a real lever of competitiveness and performance.

€220
Revenue
At the end of 2019

2,200
Employees
At the end of 2019

20
Years
of uninterrupted growth

NEW YORK • PARIS • LYON • GRENOBLE • MORLAIX • NANTES • TOULOUSE • AIX-EN-PROVENCE • MADRID • BARCELONA • LISBON
CASABLANCA • HONG KONG • SINGAPORE • AUSTRALIA • PHILIPPINES • INDONESIA • PANAMA • COSTA RICA • DOMINICAN REPUBLIC

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 35 billion events per month, and a commitment to long-term customer partnerships. Global brands such as Twitter, Airbnb, and Twilio rely on Sift to gain competitive advantage in their markets. Visit us at sift.com and follow us on Twitter @GetSift.

200+
Full-time employees

$107M
In funding

34K
Sites and apps worldwide

NEW YORK • SAN FRANCISCO • SEATTLE • DUBLIN • SINGAPORE

CONTACT US

VISEO USA
Emmanuel Deverre
Managing Director VISEO USA
emmanuel.deverre@viseo.com

VISEO Group
Hélène Sigrand
VP Marketing & Communication VISEO Group
helene.sigrand@viseo.com

SIFT
press@sift.com