FORTER®

E-BOOK

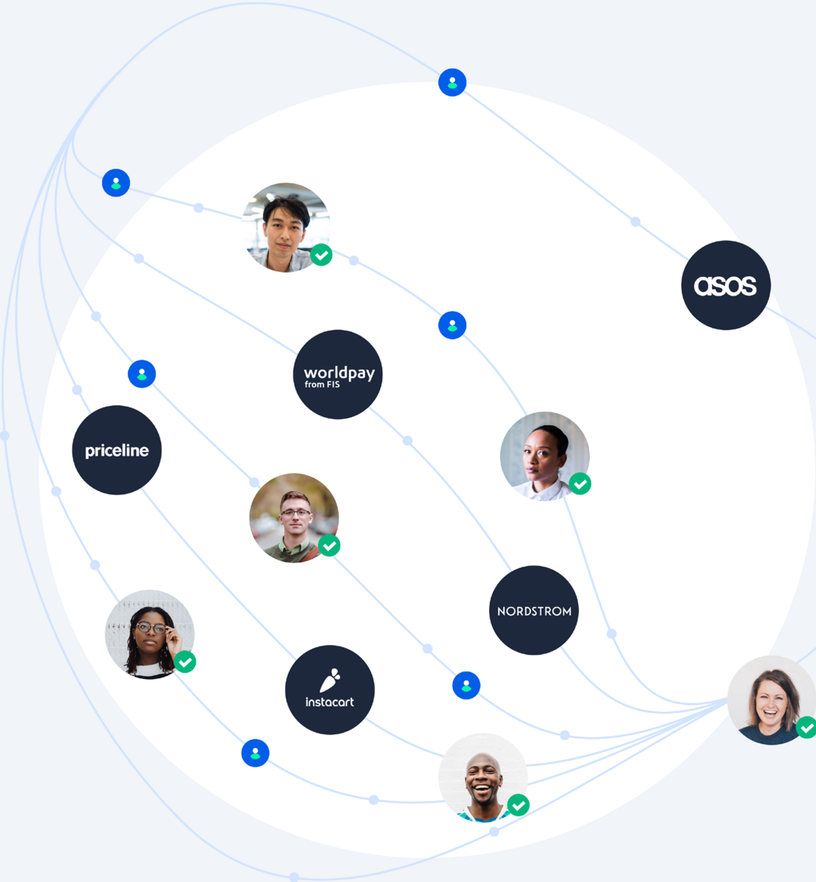
Rules-based vs. automated fraud prevention

A comprehensive guide

Index

Business beyond rules

Too many businesses still rely on rules-based systems for fraud prevention, which can't keep up with fraudsters who use modern tools like bots, device emulators, and machine learning (ML). These systems are slow to adapt to sudden changes in consumer behavior or an influx of new online users, and they can be overly punitive of your best customers. Businesses need to move beyond rules and towards a solution that automates fraud prevention.



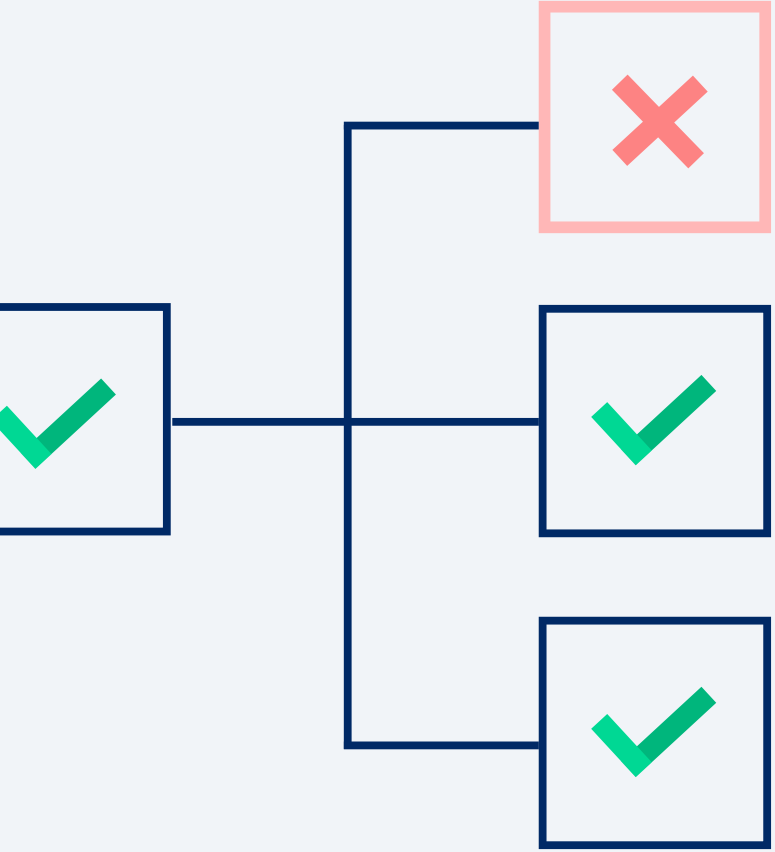
This guide explains:

Pitfalls / Some of the pitfalls of using rules-based fraud prevention solutions

Automations / Types of automation used for fraud prevention

RTFD / Why you need real-time fraud decisioning

Rules-based fraud prevention



A manual process

A rules-based fraud prevention system works as it sounds—you program rules into the system based on known instances of fraud. Each rule contains a set of conditions that the system uses to determine fraudulent transactions. If a transaction meets the conditions of a rule, the system flags it as **"fraudulent"** or **"potentially risky"** and sends it to manual review.

Traditionally, businesses would use rules-based systems to prevent fraud, and many still do so today. They still rely on rules because they are simple and easy to interpret. And because of their simplicity, creating rules-based models and validating their performance is easier to do compared to other types of models.

When a company uses rules alone, they usually wind up with a system that contains **thousands of overlapping rules**, which makes the system:

Prone to false positives / When you have a system with thousands of rigid rules, you're bound to block a high number of legitimate customers. When you reject the transaction of a genuine customer, you're also rejecting all the future purchases that the customer might have made at your business. **40% of shoppers who are falsely declined on the** first visit **won't try to buy from that site again**.

Difficult to scale / Rules-based systems **rely on manual reviews to sort out flagged transactions**, which simply doesn't scale with the growth of e-commerce. As the order volume increases, so does the number of manual reviews and human resources needed to complete them.

Reactive / Rules-based systems are necessarily reactive. **Fraud must happen AND be identified**, and only then can rules be written to try and prevent it. In the waning period between when fraud starts and the rules are implemented, there is material economic impact.

Often outdated / Rules-based systems require teams to **constantly add new rules and adjust existing rules**, which takes time to do. By the time you add or update rules, fraudsters have already altered their tactics. A system that relies on manually entering rules cannot keep up with changing trends in fraud.

To effectively prevent fraud, you need a solution that requires as little human intervention as possible, which means you need automation. **But what does automated mean when it comes to fraud prevention?**

Automated fraud prevention

There is some confusion in the market as to what automation means and how organizations should apply automation. Some companies automate straightforward repetitive tasks to boost operational efficiency. Others apply automation to complex business processes, automating them end to end.

When it comes to fraud prevention, automation comes in different forms.

Most companies use a combination of technologies to create automated fraud prevention solutions. For example, a vendor may develop a risk engine and enhance it with machine learning or create a solution

Risk engines

Some vendors provide a risk engine that predicts potentially fraudulent transactions based on a risk calculation. When you integrate a risk engine with your e-commerce system, it will provide a risk score for each transaction. Note, risk engines do not provide decisions, only scores that you must integrate into your decision process. Most risk engines focus on payment fraud, and they make calculations based on examples of known fraud. Like rules-based systems, traditional risk engines look at the characteristics of individual transactions and can't detect unknown fraud. They also can't evaluate personas or behavioral patterns over time unless they also leverage machine learning.

Machine learning

Most companies in the fraud prevention industry use machine learning because it can automatically identify patterns in massive volumes of data, including sophisticated fraud behaviors. Systems can then use that information to assess user behaviors and transaction risk. Machine learning allows systems to automate fraud detection, covering a broader set of fraud scenarios than rules-based systems. Some risk engines use machine learning to reduce the number of manual reviews needed.

While supervised and unsupervised learning have a few disadvantages, they allow companies to catch far more types of fraud and much faster than rules-based systems.

The two most common types of machine learning in fraud prevention are supervised learning (SML) and unsupervised learning (UML). Supervised learning can accurately detect known fraud types. However, you first need to train SML algorithms with examples of known fraud incidents—which means that SML models cannot detect unknown fraud. Unsupervised learning can assess transactions and user behavior in real time. Also, UML algorithms can analyze and detect patterns of fraud without needing prior fraud knowledge, giving them the ability to detect new and unknown forms of fraud. However, typical UML approaches are prone to false positives.

Artificial intelligence (AI)

Machine learning is about teaching machines to learn without being explicitly programmed. It allows machines to do tasks repeatedly, automating repetitive tasks. AI is about providing machines the ability to complete tasks that ordinarily require human intelligence, such as deciding if a transaction is too risky to be approved or what product to recommend to an online shopper.

> **Some people think that AI and machine learning are the same things—they aren't.**

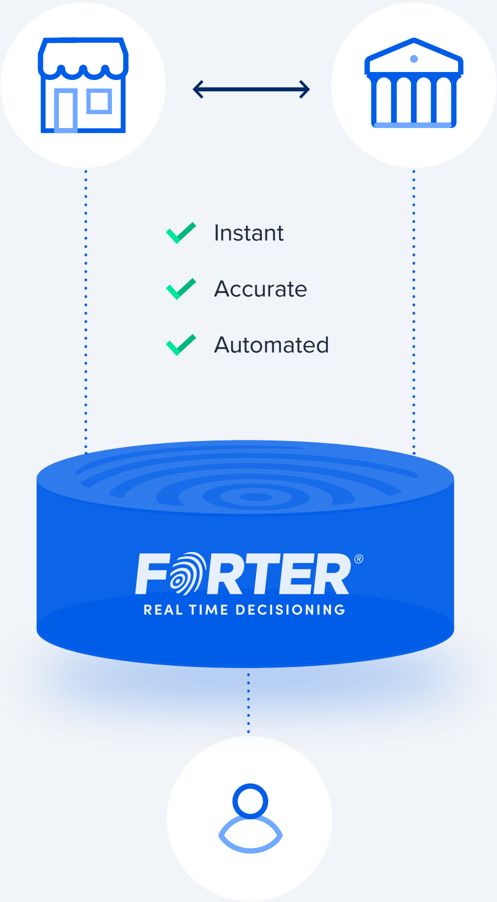
While machine learning is a subset of AI, a fraud prevention solution that uses machine learning doesn't necessarily mean it's an AI solution or performs tasks in real time. An effective fraud prevention solution makes accurate real-time decisions about transactions and user behavior—and it can't do that without machine learning **and** AI.

You need real-time decisioning

Traditional fraud prevention systems, even those that are automated, aren't designed to handle sudden changes in consumer and fraudster behavior. Between March 2020 and March 2021, there was a **500%** increase **in new online buyers** compared to the previous 12 months. We also saw the demand for convenient and fast services increase dramatically, like same-day delivery and buy online pickup in store (BOPIS). Fraudsters noticed the change in consumer behavior too—we saw a **55% increase in BOPIS fraud attacks**.

When the number of new online buyers suddenly skyrocketed, businesses with rules-based solutions saw a spike in false declines and a massive backlog of manual reviews. Companies who didn't already offer BOPIS and same-day delivery found that many consumers demanded them. However, businesses with systems that require manual reviews can't process orders fast enough to offer these services.

Companies need a fraud prevention solution that can adapt to sudden changes in behavior and make decisions about fraud at lightning speed. With real-time decisioning, you can offer fast and convenient order options to legitimate customers while preventing fraudsters from exploiting those services.



Why choose Forter for fraud prevention?

We provide a **100% automated fraud prevention** solution powered by AI and machine learning—95% of decisions are made in **under 400 milliseconds**. Our fraud models leverage personas and a global network of behavioral data, distinguishing legitimate customers from fraudsters and policy abusers.

Our platform protects your organization against fraud and abuse at every touch point of the customer journey without adding any friction. When genuine customers check out, they won't face unnecessary verification steps, unwarranted credit card declines, and lengthy manual reviews.

Our teams of fraud experts continually conduct research to curate our fraud models, keeping up with emerging fraud trends. We also build tailored models that evolve with your business, so fraud prevention always accurately reflects your current business model, service portfolio, the markets you operate in, and your risk appetite.

With Forter's automated fraud prevention solution featuring real-time decisioning, you can increase approvals and we guarantee positive outcomes. You can provide customers an exceptional experience by eliminating friction and offering fast and convenient service options.

The Network

- ✓ $200B in transactions
- ✓ A billion unique online identities

The Service

- ✓ On-demand support
- ✓ Personal performance insights

The Platform

- ✓ Instant
- ✓ Accurate
- ✓ Automated

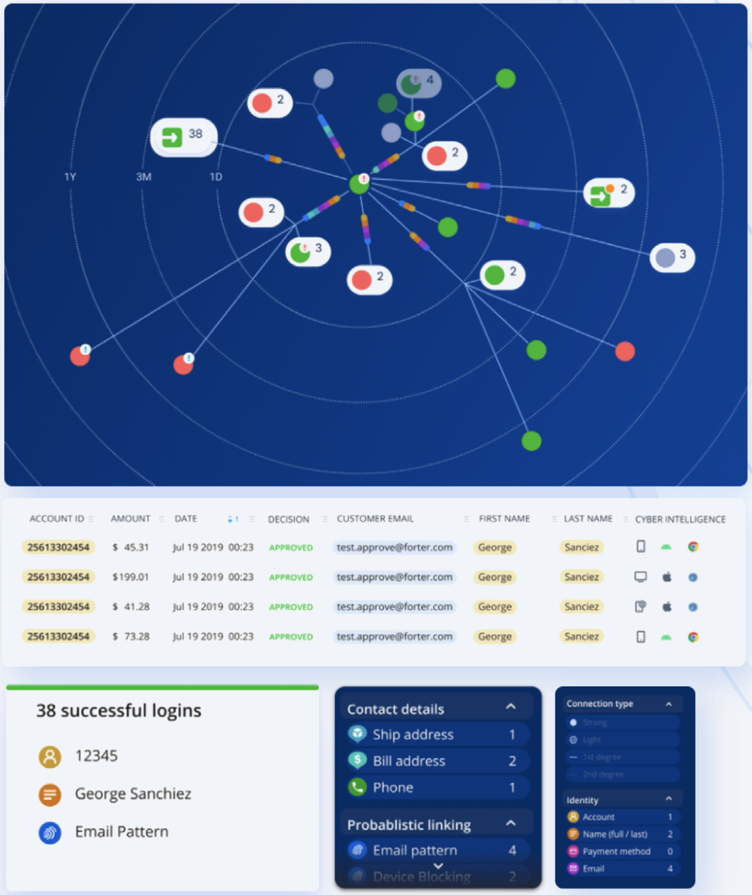
Forter’s Persona Graph

One of the most significant problems facing businesses today is bringing in new customers. Our research found that on any e-commerce site new customers are **5-7X more likely to be falsely declined** than returning customers because of a lack of data. In fact, **businesses can lose up to 75X more revenue** to false declines than to fraud.

A transaction or risk score can’t tell you if you can trust that new customer, nor can any set of rules. You need access to personas and behavioral data to determine if a new user is a genuine customer or a fraudster—**that’s the power of our Persona Graph**.

Our platform looks across our entire graph of **one billion personas** in such an interaction to determine if we know that user. If the user is known, our platform provides a precise decision. Thanks to probabilistic modeling, if the user isn’t known, our Persona Graph knows someone like them. Based on the characteristics of that similar persona, our platform can make an accurate decision about whether to accept or reject their transaction.

With real-time decisioning and our Persona Graph, businesses can accept new customers with confidence while blocking fraudsters, reducing false declines, and driving growth.



ACCOUNT ID	AMOUNT	DATE	DECISION	CUSTOMER EMAIL	FIRST NAME	LAST NAME	CYBER INTELLIGENCE
25613302454	$ 45.31	Jul 19 2019 00:23	APPROVED	test.approve@forter.com	George	Sanciez	
25613302454	$199.01	Jul 19 2019 00:23	APPROVED	test.approve@forter.com	George	Sanciez	
25613302454	$ 41.28	Jul 19 2019 00:23	APPROVED	test.approve@forter.com	George	Sanciez	
25613302454	$ 73.28	Jul 19 2019 00:23	APPROVED	test.approve@forter.com	George	Sanciez	

38 successful logins

12345

George Sanchiez

Email Pattern

Contact details	
Ship address	1
Bill address	2
Phone	1
Probablistic linking	
Email pattern	4
Device Blocking	2

Connection type

- Strong
- Light
- 1st degree
- 2nd degree

Identity	
Account	1
Name (full / last)	2
Payment method	0
Email	4

Questions to ask suppliers as you assess their solutions

Interested in automating fraud prevention? Here are some questions you should ask **Fraud Prevention vendors** as you assess their solutions.

01. Do you use both AI and machine learning?

Why you should ask this

If the vendor only uses machine learning, it means their solution is automated but may not perform tasks in real time. Many fraud detection and prevention platform vendors only use supervised learning.

Forter's answer

Forter uses both AI and machine learning so that our fraud prevention solution includes real-time decisioning.

02. How often are your fraud models updated?

Why you should ask this

Fraudsters constantly change their strategies and techniques, so you need a fraud prevention partner who continuously updates and improves their fraud models.

Forter's answer

Forter integrates new fraud patterns into our AI and ML models within hours of discovering them.

03. How long does it take your solution to start detecting fraud once it's integrated with a company's e-commerce platform?

Why you should ask this

Not all fraud prevention solutions need a lot of time to learn your system before they can start detecting fraud.

Forter's answer

Our fraud prevention solution starts detecting fraud within hours or minutes of integration with your system.

04. How many machine learning models does your company use?

Why you should ask this

You won't find any vendor with one all-purpose machine learning model that detects every type of fraud. An effective fraud prevention solution uses an ensemble of ML models, such as Random Forest, Gradient Boosted Tree, and Naive Bayes.

Forter's answer

Forter uses an ensemble of supervised and unsupervised learning models. We also use AI models.

FORTER®

Thank you!

Ready to get started?

Schedule a customized demo with an expert.

SCHEDULE A DEMO