centific

How to Fight Digital Fraud to Ensure a Safe Customer Experience

Fighting digital fraud is increasingly Job One for any business. According to Cybersecurity Ventures, cybercrime could cost businesses around the world $10.5 trillion annually by 2025.

Unfortunately, the problem is only getting worse for a number of reasons. They include:

A higher volume of online transactions creates opportunities for fraudsters to commit cybercrimes.

eCommerce is booming. In 2021, retail e-commerce sales globally amounted to an estimated $5.2 trillion, which is expected to continue, with a 56 percent increase forecast over the next few years, reaching $8.1 trillion by 2026. A higher volume of online transactions creates opportunities for fraudsters to commit cybercrimes.

Fraudsters are getting access to more tools. For example, criminals are learning quickly how to use generative AI tools such as ChatGPT to create authentic-looking emails used for phishing attacks, spam, and malware to steal money and passwords.

As a result, the cumulative merchant losses to online payment fraud globally between 2023 and 2027 will exceed $343 billion, according to Juniper Research. Therefore, it is crucial for companies to have reliable and effective fraud prevention measures in place.

Businesses have responded to the growth of digital fraud by investing heavily into technologies, including AI, to monitor the threat of digital fraud around the clock. They've also implemented processes and hired teams of fraud prevention specialists to detect fraud and protect their customers.

But unfortunately, they're viewing these crucial elements in isolation and missing out on opportunities to make them reinforce each other.

We believe the answer for fighting digital fraud is to connect the dots between people, process, and technology – what we call the virtuous circle of digital security. At the same time, businesses need to apply their investments into people, process, and technology in continuous fashion, which we refer to as the digital safety framework.

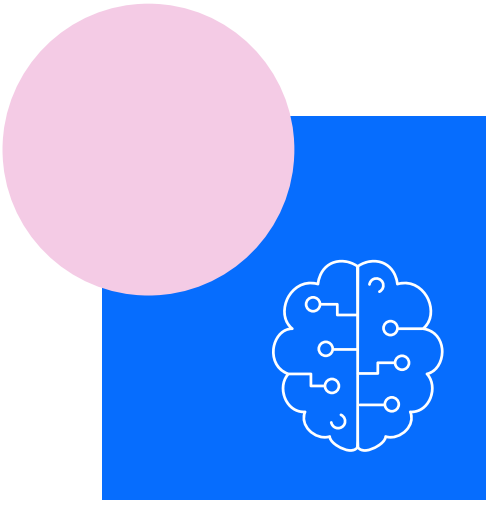
Let's take a closer look.

1

The Virtuous Circle of Digital Security

No business can succeed in the war against digital fraud without a strong investment into people, process, and technology – especially AI.

But too often, businesses are managing people, processes, and fraud detection technologies in isolation. Even worse, they're investing in one of these elements at the expense of the other – most commonly by viewing AI as a replacement for the fraud specialists who are actually needed more than ever to ensure that AI does its job. When that happens, businesses take one step forward and two steps back in the war against digital fraud. But when businesses view these elements as mutually reinforcing, they can make a breakthrough:



Artificial Intelligence

AI is a godsend for businesses to fight fraud. **AI can spot patterns of potential fraudulent activity by sifting through vast reams of data that no human being could ever possibly hope to monitor without AI.** And AI is a fast learner. Businesses are already figuring out how to use conversational AI tools to stay a step ahead of bad actors who are using the same AI to try to commit fraud.

Businesses are realizing that AI is not a one-time investment. It's a continuous one. For example, fraudsters have been figuring out how to hack facial recognition systems with photos scraped from social media profiles So, businesses are investing into AI that uses motion capture, which requires someone to move their head and neck or blink their eyes, thus making facial recognition more secure.

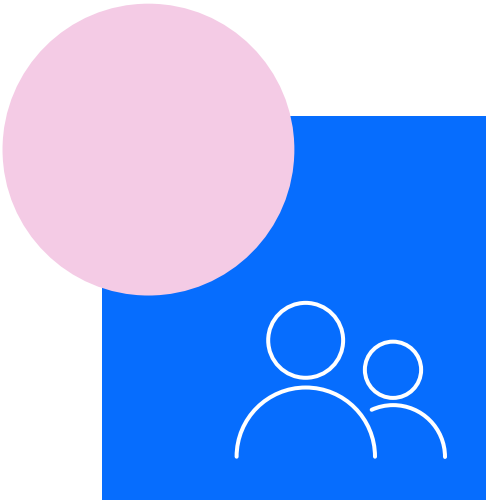
But many businesses are making a fundamental mistake with AI. They're using it to replace people instead of deploying AI with the help of people. Without people, AI has these problems:

- **It is not always right.** AI can commit false positives (reporting a legitimate action as fraudulent) and false negatives (failing to catch a fraudulent action).
- **AI can be biased** – for instance, in fraud detection, as one example, biased data and predictive models could erroneously associate last names from other cultures with fraudulent accounts, or falsely decrease risk within population segments for certain type of financial activities.
- **AI can be dated.** Fraudsters are using new techniques. AI trained on yesterday's data won't catch them.

People are needed more than ever. People are needed to train the AI to do its job.

People are needed more than ever. People are needed to train the AI to do its job. To stay in the loop to improve AI. To exercise human judgment and safeguard the customer experience when AI believes it has identified a crime and is unsure.

That and much more.



Role of People

When people remain involved to train AI, help AI make judgment calls, and then improve it, a business enjoys a much stronger customer experience while fighting digital fraud.

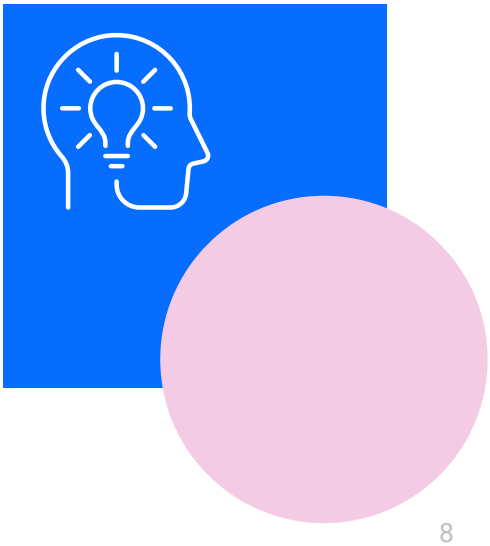
For example, let's look at how human judgment can prevent a customer experience problem from arising. Let's say a fraud detection system for a big-box retailer notices that a long-time customer is spending an inordinately large amount of money over a period of weeks using their store-issued debit card. In fact, the amounts are skyrocketing well past what the customer normally spends.

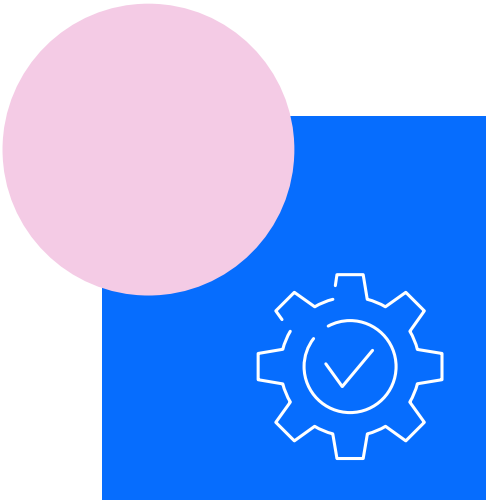
An effective AI system does its job by flagging a potential problem that human beings might have missed. But this does not mean the retailer should cancel the customer's store-issued debit card. No, **a human being is needed to analyze the purchases.** What if the customer is spending more money on baby food, toys, and clothing from the kids department? Clearly, this is a sign that the customer has become a parent, which could explain the spike.

Now, if the customer is 75 years old, the human fraud investigator probably has cause to contact the customer about the pattern of purchases. But even then, canceling the card outright might be the wrong call. What if the 75-year-old is a grandparent helping their adult kids manage through a financial need?

Without human intervention, a store might automatically shut down the debit card, which could create a major customer experience problem for a new family just when they need access to their debit card more than ever. **When people analyze the behavior against their profile of the customer – instead of looking at data in isolation – they can protect the customer experience while keeping it safe.**

People are also needed to help AI get better. This is especially true when AI fails to catch fraud. People are needed to study what went wrong – for instance, maybe the AI had not been trained effectively to catch instances when a stolen credit card to buy an item online. It needs to be retrained to improve on its mistakes.





Processes

Every business has processes in place to fight digital fraud. Those processes typically focus on dispute resolution. The challenge is making those processes work faster, more efficiently, and less expensively. This is where a stronger interplay with AI and people can help.

For instance:

- **What is the organization's process for training and then retraining AI to fight fraud?** Have those steps been baked into the entire fraud prevention protocol? Only by incorporating AI retraining as a required protocol can a business ensure that AI does its job well.
- **What is the process for following up with customers after a fraud incident has been resolved?** What kind of customer feedback model has been incorporated to make sure the business is going beyond dispute resolution and providing a positive customer experience?

The key to ensuring that AI does not commit false positives and false negatives is to train people to know what mistakes to look for and how to improve the AI model. Too many existing fraud solutions lack a feedback loop where they take learnings and feed it back to AI models. When you don't do that, you are not making AI smarter.

Only an agreed-upon process will make this feedback loop a reality, not an ad hoc experience.

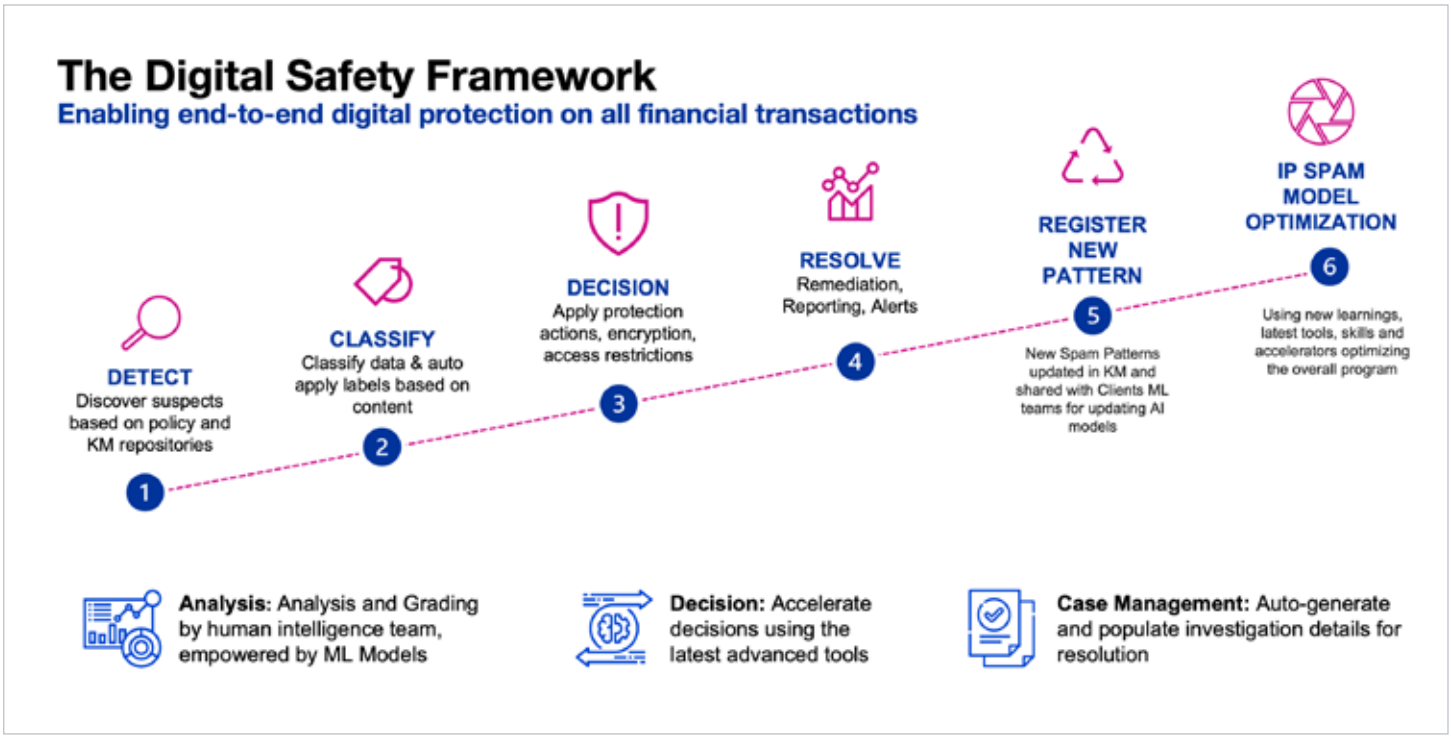
2

The Digital Safety Framework

How does a business maximize the value of this virtuous cycle of digital security? The answer is to apply these three elements through a comprehensive process of constant improvement, which we refer to as the digital safety framework.

Enterprises empowered with a digital safety framework fortify the customer journey, from authentication through post-purchase. They protect privacy and improve customer sentiment while optimizing operational costs.

The digital safety framework detects potential vulnerabilities, classifies the vulnerability according to risk score, makes decisions about fraudulent versus non-fraudulent activity, resolves vulnerability, registers the fraudulent activity by cataloging the pattern, and optimizes the operational efficiency.



Let's break down its core components.

Detect

Getting started with digital safety begins with taking stock of the strengths and weaknesses of its current approach.

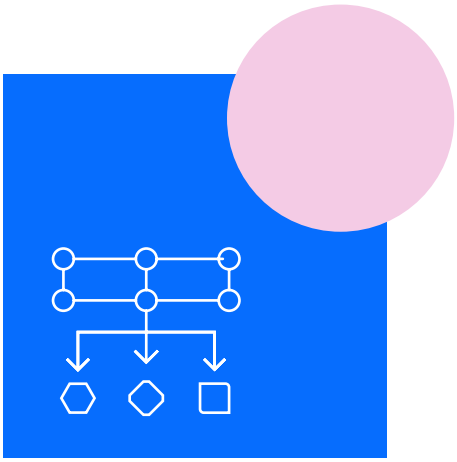
Large businesses typically have in place all the elements to fight digital fraud, and they might be ready to level up, usually with a technology upgrade. To do that, **a company first needs to understand everything that happens before, during, and after digital fraud takes place.** This includes questions such as:

The types of transactions happening across each store. What volume is being managed? What's the complete history of digital transactions occurring year after year down to the month and day?

What amount is the business losing because of fraud?

Factors such geography. Where is fraud happening at the store level and online? This gives the organization a sense of the "what" – transaction volume.

How many times was a credit card stolen compared to actual complaints received? This question helps a business understand how often AI is failing to detect fraud and incorrectly reporting legitimate transactions as fraudulent.



Classify

Once a business gets a complete picture of the "what," it's time to look more closely to detect patterns of fraud. **During digital fraud classification, the business examines all the factors cited in the detection phase to see what connections might exist between them** – for instance, whether certain stores are more likely to be victimized by more expensive fraud than others.

During classification, a business tries to **get an accurate snapshot of how fraud is investigated and resolved.** This means going step by step through the processes in place to see how effective processes are and how cost effective. For instance, how many steps does it take for a fraud detection team to act on fraud that AI failed to capture but a customer reported? What was the average cost for each incident to resolve? A business that spends on average $25 to investigate a $5 fraud is clearly not spending its money wisely.

A business that completes classification properly really understands not only the extent of its fraud problem but the efficacy of its fraud solution.

Decision and Resolution

This part of the digital safety framework really ties together the virtuous circle. At decision and resolution, a business takes into account all the information it has collected and analyzed in the previous steps to assess how to improve the way AI, people, and processes can complement each other most effectively.

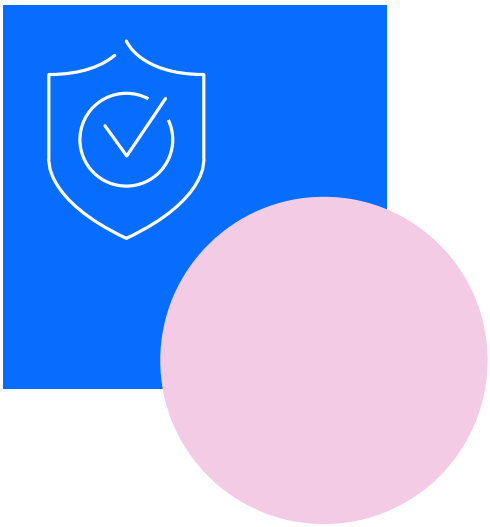
Once a business **get a complete picture of what's going on – what kind of fraud happened, how long it took, and how much was lost** – then it can examine how to improve the people and processes the next time with the help of AI.

Let's say a business realizes that AI is doing a successful job flagging outlier behavior at one store but not at another. During decision and resolution, the business finds out what specific steps need to happen in order to improve store-level performance continuously. This is done with the help of engineers working behind the scenes to with the help of an AI platform.

As noted, **AI alone won't make long-term improvements.** At the decision and resolution phases, a business involves its people to assess how to improve AI. And they'll know because a process was in place to do that.

The benefits of adopting a digital safety framework include:

- **Safeguard customer accounts:** Secure business from scams and reputation losses by defending against fake account creation, account takeover, and fraudulent account access.
- **Improve revenue acceptance:** Financial institutions may now improve transaction acceptance rates with insights that help balance revenue opportunity against fraud loss and checkout friction.
- **Protect revenue losses from discount and return fraud:** Identify anomalies and potential fraud to quickly act to reduce revenue impact.



3

The Centific Approach

Our approach to combating fraud consists of an **AI platform** that detects and classifies fraud complemented with a **fraud squad of expert analysts** equipped with a very high emotional intelligence, ensuring digital safety throughout your ecosystem.

The AI Fraud Protection Platform creates a circle of trust across the customer journey, from account protection and purchase protection, while protecting your business through loss prevention. Account protection mitigates account takeovers and purchase protection correlates the transaction patterns of potential bad actors performing fraudulent activity. Loss prevention detects anomalies throughout the transaction history, mitigating financial loss.

Dynamics 365 Fraud Protection Implementation, Integration + Manual Fraud Review Delivered by Centific

Our fraud squad can create business transaction workflows for increased operational efficiency to transform your organization. By infusing artificial intelligence with emotional intelligence, our fraud analysts have accelerated dispute resolutions, improved the win rate for chargebacks, and assessed fraudulent activity with one of the lowest false positive/false negative metrics in industry.

Our human-in-the-loop approach makes it possible for AI-powered fraud platforms to detect, prevent, and resolve digital fraud events faster, in turn reducing financial loss. The Centific augmented intelligence framework encompasses people, process, and platform pillars to operationalize anti-fraud efforts at scale.

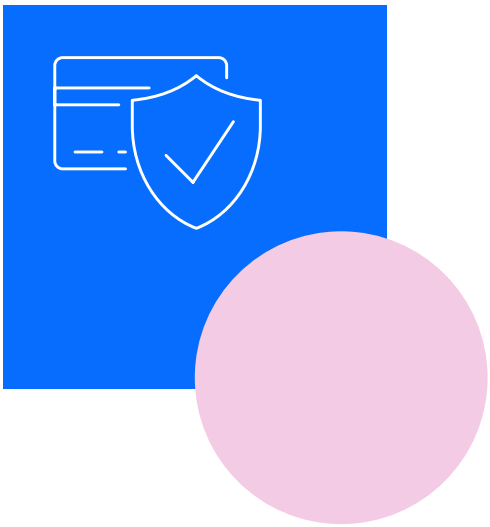
This approach accelerates efficiencies while delivering value through agility. By unifying a wide range of data sources, our cognitive decision-making platforms **reduce risk, increase efficiencies, and enable real-time monitoring.** By streamlining fraud frighting initiatives, businesses deliver a better customer experience and safeguard their bottom line.

Digital Safety in Action

Our client was facing challenges to prevent fraud in sign-up and purchase on its online store that processes $10 billion+ of transactions in a year. Criminal hackers were using stolen credit cards or compromised accounts to make unauthorized transactions.

Using machine learning, Centific **redesigned risk-scoring rules and set up end-to-end system integration with eCommerce, ERP, and databases** incorporating MLOps pipelines. Our work spanned data collection, data curation, machine learning modeling,performance evaluation, data visualization, advanced monitoring, and alerting mechanisms to meet fraud business KPIs.

Results: we significantly increased the decision-making accuracy of fraud recognition models and **prevented more than $1 billion in potential fraud loss.** The bank transaction acceptance rate also significantly **increased saving an additional $10 million.**



4 Conclusion

Without question, fraudsters are getting more resourceful, and the problem of fraud is not going to go away. But businesses possess scale and resources to fight digital fraud effectively. All the pieces are in place – people, processes, and AI. It's time for businesses to make a breakthrough by making these elements flourish together.

About Centific

Centific is a global digital and technology services company. We design, build, and optimize human-centric intelligent digital platforms. Our core capabilities are in data, intelligence, experience, and globalization. Learn more at centific.com