

White Paper

From fraud detection *to prevention*

Implementing robust fraud prevention systems for today's increasingly digital and virtual world

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Executive summary

In an era where remote work and rapidly developing artificial intelligence (AI) technologies are redefining how and where we do business, fraud is a rapidly growing concern for global executives. Considering 51% of global organizations[1] experienced fraud in the past two years — the highest level in 20 years of research — it's easy to see why.

With so much unprecedented change, it's becoming increasingly difficult for leaders to safeguard business processes, protect sensitive data, and streamline measures to mitigate fraud incidents, often leading to costly consequences. Indeed, over half[2] of organizations who experienced fraud (53%) also experienced financial losses in the ballpark of $1 million to over $50 million.

In this brief, we'll explain why a new paradigm is required when it comes to successfully mitigating fraud, exploring what a holistic fraud prevention approach looks like, both in theory and in practice.

Key Takeaways

- Over half of organizations experience fraud, resulting in financial losses and negative business outcomes.
- AI-powered and remote fraud, coupled with a volatile economic climate, has led to an uptick in fraud incidents that's expected to continue.
- Only a holistic fraud prevention system that incorporates the right processes, controls, and tools can successfully move from detection to prevention.

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Fraud: A growing problem with a remote, AI-powered workforce

All companies handling sensitive data are at risk for fraud. Unfortunately, the economic volatility of the past few years has led to a broader trend of increasing fraud rates[3], especially when it comes to areas like financial fraud. In fact, 69% of global executives and risk professionals expect financial crime risks to increase[4] over the next year, particularly in areas like cybersecurity and data breaches.

Given the current climate, leaders need to understand where fraud attempts are coming from — whether from external or internal perpetrators — and how rising technologies like generative AI are exploiting weaknesses in existing fraud detection systems.

Fraud attempts fueled by AI

With the advent of AI-powered fraud[5], knowledge of risk areas and proactive measures to prevent fraud are becoming more important than ever.

For example, emerging tools like ChatGPT are exposing organizations to previously uncharted risks. A new study[6] found 15% of employees regularly use generative AI like ChatGPT at work, with 43% inputting internal business data and 12% sharing personally identifiable information (PII) with the tools. That data could end up in the hands of competitors at best, fraudsters at worst.

No matter the tactic, fraud is becoming an increasing risk for organizations, both internally[7] and externally. While fraud from internal perpetrators is down since 2020, both external fraud and collusion between internal and external actors have increased[8] since 2020. According to Jeff Schilling, Chief Information Security Officer (CISO) at Teleperformance, mitigating fraud starts by identifying and understanding fraud risks.

> "Fraud, like security, it about risk management. You have to identify the risks, build a mitigation plan to address those risks, and then apply those mitigating steps to lower the residual risk."
>
> **Jeff Schilling, CISO, Teleperformance**

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Three of the most common types of fraud[9] include cybercrime, customer fraud, and asset misappropriation. For organizations whose employees handle sensitive data, credit card fraud, product shipping, and data breaches are also top concerns. Each of these can have a large impact on businesses if not recognized and mitigated correctly.



Common types of internal fraud

Credit card fraud:
When an employee copies credit card numbers and uses them to purchase online.

Product shipping:
When an employee ships products to an accomplice's address.

Data breach:
When an employee collects social security numbers and resells them to an accomplice.

Illegitimate benefit:
When an employee uses client applications for personal gain, such as inflating hours worked.

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

The business impact of fraud

Fraud is costly, and not only in terms of financial loss. Fraud can result in lost trust, leading to less credibility from customers and decreasing morale from employees. According to Schilling, fraud prevention lies at the heart of maintaining trust in the relationships that matter the most to your business.

In short, fraud has a disproportionate negative effect, resulting in both tangible and subtle losses. For example, fraud can have an impact on both internal and external business outcomes[10], leading to consequences like regulatory fines, increased incidents, and brand or reputational damage in the eyes of customers.

"When you lose trust, that's when you start losing revenue — people start going to more secure solutions. Everybody should have a fraud management program to protect revenue. Otherwise, they lose the trust of their customers which inevitably impacts revenue."

5 negative effects of fraud[11]



Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Where fraud detection falls short

Detection is no longer a sufficient strategy[12] when it comes to fraud. Without tools, processes, and controls in place to anticipate and mitigate attacks in the first place, organizations leave themselves a step behind would-be fraudsters who can leverage emerging technology to their advantage.

This is especially true in times of economic turmoil. For example, 70% of organizations[13] experienced new incidents of fraud and increased fraud risk in the wake of the COVID-19 pandemic. Digital operations have introduced new levels of risk in areas like employee misconduct and platform risk — two common risk areas still prevalent today among hybrid and remote work environments.

Simply put, tools, processes, and controls that were sufficient to detect incidents of fraud may have been sufficient in pre-pandemic, pre-generative AI years. Today, however, tools that aren't proactively preventing fraud while putting the latest emerging technologies into use are at risk of falling into obscurity.



Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

A holistic system for fraud prevention

Whether it's protecting sensitive data in a work-from-home setting or ensuring employees aren't feeding sensitive data into generative AI tools, the methods and means used to protect against fraud need to become at least as sophisticated as the tools now empowering fraud attempts. With a holistic fraud prevention system in place, organizations can prepare for the inevitable uptick in attacks enabled by AI and other emerging technologies.

What does a holistic fraud prevention system look like? It should accomplish each of the following:

- **Assess processes** across the company to identify risks.
- **Create controls** to mitigate problems related to fraud attempts for both processes and the workforce.
- **Utilize tools** to promptly respond and manage threats, and ultimately provide employees with information and tools to avoid and report malicious activities.

"If you don't take a methodical approach like this, then you become one-hundred-percent reactive and you're going to have increased fraud as well as the inability to detect it.

Schilling explains. "The worst thing is when somebody else tells you you've got a fraud problem."

6 benefits of holistic fraud prevention

1. Prevent fraud and cyber attacks before they happen.
2. Increase operational cost-savings.
3. Improve the entire business ecosystem to safeguard sensitive data.
4. Protect business data whether employees are on-site or remote.
5. Protect revenue and client churn.
6. Use real-time system alerts to detect data breaches and fraud attempts.

At Teleperformance, we use a seven-step system that incorporates processes, controls, and proprietary tools to proactively prevent fraud incidents as well as detect them in real time.

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Teleperformance's 7-step fraud prevention life cycle

First and foremost, Teleperformance constantly updates and refines our fraud risk management system based on emerging threats and industry best practices. Today, our seven-step framework integrates cutting-edge technologies, such as AI-powered fraud detection systems and biometric authentication, to bolster our fraud risk management process.

This proactive approach ensures that we stay ahead of evolving fraud tactics, providing our clients with a secure and reliable environment. Let's dive into each of the seven steps to examine a holistic system in more depth.

1. Green start risk assessment

Before we launch any services together with a new client, we conduct an initial assessment to identify five typical delivery risks associated with fraud.

These initial fraud risks include:

- There's no foolproof way to identify the customer, allowing for possible impersonation fraud risk.
- Access to the customer relationship management (CRM) software is allowed when employees are not on a customer call.
- Financial information is exposed during a call.
- Employees can make changes to the account without notifying the customer, allowing for possible credit card fraud and illegal refunds.
- Metric manipulation is possible, including modifying average handling time or other performance indicators.

If any major risks are identified in this stage, we send a letter to the client identifying any areas of exposure along with recommendations for best practices to mitigate those risks.

2. Full security risk assessment

After clearing initial risks, we then conduct a comprehensive evaluation of over 200 registered risk items within the first 120 days in order to prevent service delivery fraud. Our in-depth checklist includes risk areas compiled from over a decade of experience, examining each and every area where we've seen fraud happen before or where potential fraud risks may arise.

Copyright © 2023 Teleperformance SE All rights reserved
Complete or partial external use or reproduction is strictly forbidden.

3. Risk mitigation

Next, we organize potential risks into one of three categories: Risk for Teleperformance to address, risks that need to be addressed together, and risks for the client to address in their own applications. We then communicate these existing client service delivery risks for visibility and resolution along with implementing mitigation controls for each of the risks under our domain.

4. Fraud analytics monitoring

After our initial identification and mitigation controls, we implement a variety of technologies and tools to detect and proactively prevent fraud, such as fraud analytics monitoring.

Our fraud analytics monitoring service can analyze client data to detect everything from individual violations (employees making unauthorized changes on accounts) to systemic violations (multiple violators working under the same supervisor, for example). These tools can even trace violations back to training groups, specific trainers, and other connecting factors that can either root out bad actors or bad training leading to errors.

5. TP Protect insider threat tools

Our proprietary tool, TP Protect, enables us to write customizable detection rules and see screen recordings of potential fraudulent incidents. For example, when an employee inputs certain keystrokes (such as a social security number), TP Protect will trigger a screen recording of the employee's activity for 15 seconds before and 15 seconds after the activity stops.

Similarly, our TP Wallet platform provides a safe and compliant softphone and web phone solution to secure credit card payments during calls by implementing digital AI assistance, preventing sensitive data from reaching employees in the first place.

6. Global ethics hotline

Fostering a culture of honesty is just as important as having tools to prevent and detect fraud. Our global ethics hotline encourages other employees to "see something, say something" by providing anonymous reporting alongside rewards for creditable reports of fraud or mismanagement.

7. Global incident response team

Lastly, when incidents do occur, it's vital to nip them in the bud and then learn from them. We have a 24/7, 365-day a year fraud investigation team with multilingual capacity to manage and report fraud incidents if they occur. Our investigators then work with HR to provide a report and investigate the incident fully.

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Case studies: Holistic fraud prevention systems in action

By applying Teleperformance's seven-step system for fraud prevention, organizations across the globe reduced malicious attempts and completely cut off employee fraud attempts in a work-at-home setting.

Safety frameworks blocked 115,000+ malicious attempts

Across 20 global clients in multiple industries, Teleperformance was tasked with safeguarding information and detecting malicious activities as well as fraud attempts among the internal workforce.

Challenges

In order to achieve our clients' goals, Teleperformance needed to create a safe and trustworthy ecosystem that included the following:

- Controls for preventing malicious activities
- Training to coach employees on safeguarding information
- Streamlined processes for handling sensitive data



Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Our approach

Our team implemented TP Protect, our proprietary tool that prevents data breaches and fraudulent attempts by capturing real-time workforce system activity inside a governance model ensuring business safety on-site and remotely.

We specifically applied TP Protect to streamline alerts on product/shipping address edits, abnormal number of searches in client applications, and shared credentials. Our framework included the following processes and controls:

- Conduct process assessment to identify patterns and outliers.
- Define secure rules to automatically trigger when suspicious activities occur.
- Cross-reference data alerts with external databases, if necessary, to validate employee personal credentials.
- Escalate critical alerts to the security operations center (SOC) for review.
- SOC team provides proof of attempted fraud, supporting human resources in discussing the case with the employee.
- Provide a coaching session, if needed, to prevent contract termination.
- Review processes to streamline improvements based on data-driven insights.

Benefits

After implementing TP Protect across these 20 organizations and following the above framework, we achieved the following benefits:

- 20 safety rules were implemented across monitored clients, on average.
- 51 coaching opportunities for experts were identified.
- 4 specialist contracts were terminated for lack of security compliance.

In total, our holistic process for fraud prevention blocked over 115,000 fraud attempts, moving our clients from a fraud detection to a fraud prevention framework.

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Elimination of fraud attempts by remote workers

A U.S. tech provider for restaurant automation and off-premise solutions asked Teleperformance to help them implement additional security measures to prevent the risk of transactional fraud.

Challenges

Our client's work-at-home (WAH) operation was at risk of transactional fraud. They needed to protect sensitive customer information in every transaction as well as ensure strict adherence to Payment Card Industry (PCI) compliance policies.

To meet these needs, Teleperformance needed to deliver a reliable and secure payment channel that met all PCI requirements.

Our approach

Our team implemented TP Wallet, our safe and compliant softphone and web phone platform that secures credit card payments during calls by protecting sensitive information from expert exposure and preventing possible fraud attempts through data breaches.

We applied TP Wallet to connect the multiple payment gateways and secure our client's transactional environment. Our platform included the following processes and controls:

- The highest level of data security and protection by adhering to PCI data security standards.
- Integration with the client's telephonic platform, enabling smooth and efficient operations.
- An additional layer of security and privacy to prevent workforce access to sensitive information.
- Credit card information entry using either the keypad or voice.

Benefits

By adding TP Wallet to their tools in their fraud prevention toolbelt, our client was able to achieve:

- 100% reduction in fraud attempts during transactions
- 100% reduction in possible penalties charges due to PCI non-compliance
- ~4% increase in gross margin achieved from cost savings with a remote work operation

In all, our client's safe and compliant work-at-home operation resulted in a 100% elimination of fraud attempts, protecting sensitive customer data and allowing for streamlined business operations.

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Fraud prevention starts with preparation

In conclusion, fraud is an evolving and increasingly difficult practice to prevent. The old paradigm of detection-first fraud systems won't be enough to deter incidents in an AI-powered world with a remote workforce. In order to mitigate financial and reputational losses associated with fraud incidents, leaders must adopt a holistic fraud prevention system that incorporates the latest in cutting-edge technologies and practices.

By putting the right processes, controls, and tools to use, organizations can get ahead of fraud upswings in times of economic volatility and stay prepared for any incident that might come their way in the future.

How to get started

Partnering with an external expert who incorporates a holistic system for fraud prevention can shortcut the learning curve and apply an already-proven model to mitigate threats. Teleperformance's fraud prevention life cycle is one such system that can improve existing systems or kickstart the growth of your own fraud prevention practice.

Learn more about Teleperformance resources to support fraud prevention by contacting a representative today.

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.

Endnotes

1. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

2. Ibid.

3.https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

4. https://www.kroll.com/en/insights/publications/fraud-and-financial-crime-report

5.https://www.forensicstrategic.com/four-strategies-your-business-can-use-to-fight-ai-powered-financial-fraud/

6. https://cybernews.com/security/workers-regularly-post-sensitive-data-into-chatgpt/

7.https://www.teleperformance.com/en-us/insights-list/white-papers/internal-fraud-the-most-pervasive-security-in-organizations/

8. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

9. Ibid.

10. Ibid.

11. Ibid.

12. https://www.finextra.com/blogposting/23975/fraud-trends-in-2023

13. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Copyright © 2023 Teleperformance SE. All rights reserved.
Complete or partial external use or reproduction is strictly forbidden.


DATA SECURITY