Ovum
TMT intelligence | informa

Enterprise Case Study: Driving Innovation in Payment Fraud Detection and Prevention through Analytics

How Poste Italiane improved its payments security capabilities with multilayered data analytics

Publication Date: 01 Aug 2017 | Product code: IT0059-000117

Gilles Ubaghs

Summary

Catalyst

All payment issuers globally face a myriad of challenges when it comes to reducing the risk of fraud. While new technologies, channels, and payment tools undoubtedly open up significant opportunities for transaction and customer growth, these same opportunities also present new threats to customer and business security. Issuers are faced not only with growing compliance requirements, but also with new fraud attack vectors constantly emerging and the need to identify problematic transactions in an increasingly crowded stream of transaction data. The risk of false positives only compounds the problems that fraud poses, leading to lost transactions (and angry customers), even where no malice was ever intended.

This case study shows how Post Italiane was able to modernize its fraud detection and prevention capabilities to meet the needs of its unique payments portfolio. Post Italiane partnered with TAS Group to develop Plus2Fraud (PROF), a next-generation fraud detection and prevention platform that helps reduce false positives and improve fraud detection through the use of analytics.

Ovum view

Fraud and security is a perennial issue for payments providers across the value chain. Although not a new issue for payments providers, it is a continually evolving one, made more challenging by the rapid diversification of payment tools and channels. There is no single point solution to all fraud and security challenges in payments, and likely never will be. As such, multilayered approaches that make use of the latest array of predictive analytics and data-driven decisioning will prove critical in the near term. Central to the success of any security solution is ensuring that capabilities cater to the needs of payment providers, merchants, and consumers alike. This means limiting the impact on the transaction process itself and understanding the nuances of the local business and regulatory environment, while also ensuring an improved level of security.

Key messages

- Poste Italiane, via BancoPosta, wanted to improve its payments security capabilities after significant increases in fraud, particularly around its prepaid card top-up transactions.
- Poste Italiane partnered with TAS Group to develop and deploy the Plus2Fraud (PROF) platform. Poste Italiane's partnering decision was strongly influenced by TAS Group's understanding of BancoPosta's technology infrastructure and local regulatory considerations.
- PROF is a predictive analytics–based tool that centers on two primary modules, SCUDO and BASE, designed to act during and post transaction. While maintaining separate rules, the outputs of both can influence each other, leading to a refinement in capabilities.
- By adding analytics to its multilayered payment security stack, Poste Italiane has improved its fraud detection and prevention capabilities and is now exploring similar solutions for anti-money laundering.

Recommendations for the payments industry

Recommendations for enterprises

Analytics can add intelligence to multilayered solutions

The use of predictive analytics has the potential to generate a much more thorough view of the evolving nature of payments security and fraud issues. However, much of this data is not being deployed effectively to help ameliorate fraud prevention strategies. For most payments organizations, including issuers and merchants alike, a balance needs to be struck between stopping fraudulent transactions as quickly as possible and avoiding false positives on legitimate transactions. Achieving this will require a heavily data-driven approach to gain a better understanding of consumers, down to the individual level, to better detect what is and is not normal or suspicious behavior.

While each layer of security adds further checks and balances, connecting these layers into a more data-driven feedback loop could help to refine fraud capabilities over time. An integrated, real-time feedback loop can enable fraud systems to augment subsequent authorization decisions. As payments fraud inevitably becomes more complex, it will likely prove more effective and operationally efficient to continually improve the capabilities of each layer, rather than simply adding more layers to the overall fraud and security stack. In essence, this boils down to a need to work both smarter and harder.

Recommendations for vendors

Configurability is everything in payments fraud

All issuers and payment providers operate in complex environments and in most instances are faced with the challenge of balancing their technology capabilities, their business goals, and local regulatory and compliance requirements. As the payments market evolves, the particulars of most organizations are only becoming more complex. Finding an off-the-shelf solution that is an exact fit when it comes to fraud and security capabilities is becoming increasingly challenging, if not impossible, for most enterprises.

As such, it is critical that vendors design their solutions and services with a focus on modular design and strong configuration capabilities. This also extends to implementation and development capabilities over time. Regulation and compliance requirements will evolve, as will the underlying payment tool and channel environments. This means that the solutions and services that are the most adaptable to enterprise users' environments, both now and over time, will find the most success longer term.

Deploying predictive fraud prevention capabilities to reduce losses and increase compliance

Setting the business context

Rising payment fraud levels are driving innovation in detection and prevention

To counteract rising levels of fraud, the payments industry has been continually evolving fraud prevention tools and services, in most instances focusing on specific payment types or channels. Hence, in recent years the introduction of EMV on cards for use at the POS has led to a dramatic decrease in levels of cloned and counterfeit cards being used in EMV-compliant regions. Fraud, however, is not a zero-sum game, and advances in preventing fraud in one direction tend to be followed by rises in fraud in other directions.

While preventing fraud is a necessity, payment providers are also faced with the challenge of not accidentally blocking legitimate transactions. False positives are a major hurdle for issuers and merchants alike and not only lead to lost sales but also run the risk of reducing trust in, if not outright abandonment of, any particular payment tool. Furthermore, in many instances, payment fraud prevention strategies that place too many hurdles in front of legitimate consumers tend to lead to high levels of shopping-cart abandonment and customer frustration. This in turn can lead to merchant abandonment of a specific fraud prevention or authentication tool, and subsequently leave an opening for would-be fraudsters.

To add to these competing needs, payment providers are also faced with a growing array of regulatory and compliance requirements in terms of data and payment security. These regulatory burdens can be particularly high for specific tools most at risk of fraud, such as prepay and cross-border P2P transactions, both of which maintain high anti-money laundering (AML) and know-your-customer (KYC) requirements.

The payments market is, at heart, a local market, and while all regions face the same pressures as described above, the local context and specifics of the regulatory and infrastructure environment mean that each country is unique, and finding a truly off-the-shelf solution is challenging to say the least. As a result, growing numbers of enterprises are now turning to new fraud prevention and detection technologies that are well suited to their specific payments environment and meet the needs of both their customers and local regulators.

Poste Italiane, one of Europe's largest issuers, needed a better fraud solution

Via its BancoPosta division, Poste Italiane is one of Europe's largest issuers (especially with regard to prepaid cards), with more than 40 million cards in issue. It also operates other payment services, including its popular mobile platform. Alongside payments products, Poste Italiane offers customers a broad range of financial services, ranging from savings and insurance through to exchange brokerage services and the promotion and placement of loans granted by banks and financial intermediaries.

After several years of continual rises in its levels of fraud, particularly within its prepaid card top-up capabilities, Poste Italiane began to search for a new fraud prevention and detection solution in 2013 to help reduce fraud rates and improve efficiencies within its internal fraud security teams. Rather than any specific single tool, Poste Italiane was interested in improving its capabilities in both fraud prevention, to stop questionable transactions during the payment process itself, and fraud detection, to identify fraud more accurately post transaction, after it has occurred.

In light of Poste Italiane's unique market positioning and product portfolio, it operates a highly complex and heavily customized infrastructure across its financial services capabilities. As a result of this complexity, most off-the-shelf products were not immediately capable of meeting Poste Italiane's needs in delivering a suitable fraud prevention capability that could be easily integrated into its existing architecture.

The role of ICT/services in solving the problem

PROF is a predictive analytics–based tool for fraud prevention and detection

After some initial investigation of other solutions, Poste Italiane decided to partner with TAS Group to develop a new tool from the ground up, due in large part to TAS Group's long-standing relationship with Poste Italiane and understanding of its infrastructure. Poste Italiane felt that TAS Group had a strong understanding of not only BancoPosta's technology but also the broader Italian business and regulatory landscape.

In 2015, Poste Italiane made a formal request for a proof of concept (PoC) on the use of predictive analytics to help combat fraud within the domain of prepaid card top-ups. From this initial PoC, TAS Group developed its Plus2Fraud (PROF) platform, which offers a multilayered solution to tackle fraud during the transaction itself and for post-transaction fraud detection and dispute resolution. Outputs from the two layers of the platform can be fed back into the underlying transaction rules of each layer and produce a more finely tuned fraud prevention and detection capability.

The PROF platform consists of two modules that operate independently but complement each other, as described above. The first module, known as SCUDO, acts in real time during the transaction process. Its functions include verifying whether a card or cardholder is blacklisted, operating rules based on the data of the transaction itself without recourse to past history, and prevention modules capable of identifying and analyzing fraudulent behavior. Detected in this way, questionable transactions can be identified, transactions stopped, and cards blocked until necessary checks take place.

PROF's second module, BASE, serves as a monitoring unit to detect fraud, and while fed by the authorization process, detection is based on a broader post-transaction stream of data. Unlike SCUDO, BASE considers a wider range of dynamic transaction data, including the history of the card and the cardholder. BASE offers two types of detection mode, centered on prepaid card reload top-ups and transactions, respectively. Using BASE, each transaction is given a risk score, and when these scores reach a predetermined threshold, a formal fraud case investigation is instigated, and chargeback management can occur as required. BASE is designed not to interfere with the authorization process or slow wider customer operations.

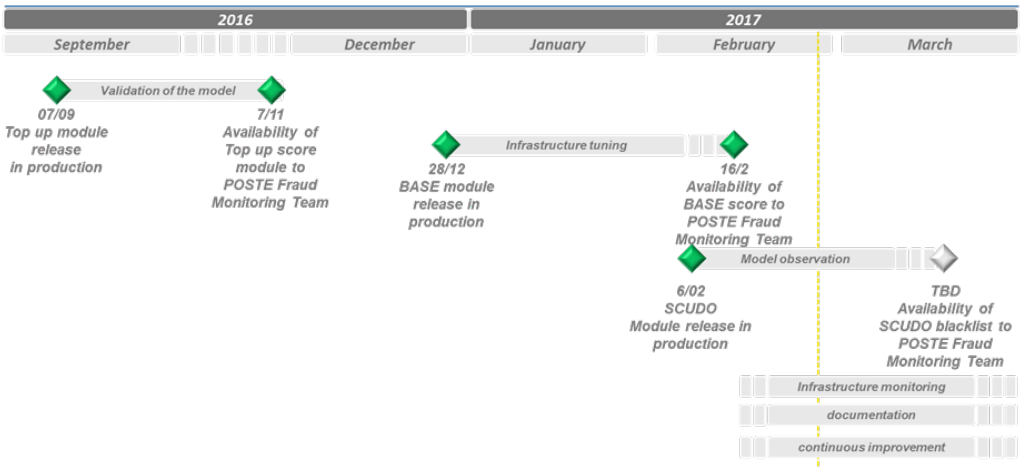
Compliance requirements shortened the development time of PROF

Poste Italiane first started experimenting with predictive models in 2015, but the regulatory requirements of the EBA for Chapter 10 compliance shortened the overall development time for rollout. These new requirements included fraud detection and transaction blocking before a payment service provider authorizes a transaction, customer behavior analysis, and a need for transaction screening and evaluation to occur in an "appropriate" time frame so as to not unduly delay the transaction. The need to meet these new requirements led to the formation of a taskforce joint working group between BancoPosta, the IT department of Poste Italiane, and TAS Group.

Implementation of PROF involved a three-stage process. Phase one was the release of the "Ricarica" predictive model, a component of BASE centered on prepaid top-up fraud detection. Ricarica was first released in September 2016 and was open to the monitoring center two months later, in November. This was followed by the BASE predictive model for all transactions types (i.e., online, ATM, and POS), with an initial release in late December 2016 and a full production rollout in February 2017. The final SCUDO model was released in February 2017 and was open to the Poste Italiane monitoring center in mid-2017.

According to Poste Italiane, the implementation went very well, and this was aided by TAS Group's understanding of both its technical environment and specific regulatory needs. While challenges did occur, they did not lead to any delays in the timeline, because TAS Group was open about its development approach and worked in partnership. This was more than simply configuring an out-of-the-box solution; it was perceived as a new and innovative way to approach a deep payments problem for the business.

Figure 1: Implementation timeline



Source: TAS Group

Outcome assessment

It remains too early to measure what precise volume of fraud PROF has detected and prevented overall, but initial reports from Poste Italiane suggest a significant improvement in security capabilities. Poste Italiane has run test scenarios against historic blocks of transactions, and it has proven more adept at accurately scoring known fraud events than the previous solution. Initial testing of the platform suggests that 67% of fraud instances could be intercepted by the predictive model alone, while the remaining third were identifiable from deterministic rules and/or a combination of predictive and deterministic functionality. The risk scores produced by PROF are fed into web interfaces for the fraud detection team at Poste Italiane, and initial feedback has also been positive. Based on the success of PROF, Poste Italiane is now exploring with TAS Group the potential to develop a similar solution for anti-money laundering (AML) capabilities.

While its security capabilities have improved, Poste Italiane admits that the solution requires a slightly different skill set than most traditional fraud prevention tools and services. The data that is input into the predictive model can have a significant impact on the transaction management rules, particularly when considering which time frames are being looked at. In turn, the outputs from these predictive models can have repercussions in other areas of Poste Italiane's operational stack. As a result, Poste

Italiane feels that strong data management and data analysis capabilities will become more crucial over time.

Although it was initially developed in conjunction with Poste Italiane, PROF has now been fully productized as part of TAS Group's Cashless 3.0 platform.

Lessons learned

Build to meet local needs

The technology infrastructure of any enterprise will have its own idiosyncrasies and complexities that are unique to that business and its operating environment. These include the legacy infrastructure in use, the regulatory environment, and the broader technology and business roadmap on where organizational priorities lie. In the case of payments, this includes the domestic competitive environment, local regulations, and even customer payment habits, which can vary wildly even between neighboring countries. Developing technology strategies and infrastructure is made significantly easier when vendors and enterprises operate from a similar vantage point to understand the nuances of the local environment.

Global technology trends are impacting enterprises and vendors alike in a myriad of ways, but the reaction in every instance is ultimately a localized decision and process. Understanding these local requirements and considerations is crucial in adapting to global trends effectively.

Ensure that each layer is designed to improve and reinforce the others

As described above, multilayered solutions are now a fairly standard practice when it comes to payments fraud prevention. However, by linking these layers together using predictive analytics, the rules guiding transactions can be fine-tuned, improving the overall effectiveness of the solution. Similar approaches have applications across the enterprise IT environment. While many organizations remain product-led, switching to a more outcomes-based model, whereby layers of the broader technology stack feed into and impact each other, has the potential to lead to more widespread operational improvements.

Appendix

Methodology

Ovum Enterprise Case Studies leverage in-depth interviews with key enterprise stakeholders as well as a review of any available documentation such as strategic planning, RFP, implementation, and program evaluation documents.

Further reading

Enterprise Case Study: Modernizing Higher Education Payments for the Twenty-First Century, IT0059-000074 (October 2016)

Enterprise Case Study: Bank Zachodni WBK Mobile Wallet, IT0003-000687 (April 2016)

Ovum Decision Matrix: Selecting a Card Management System Platform, 2015–16, IT0059-000031 (October 2015)

Ovum Decision Matrix: Selecting an Electronic Retail Payment Switch Platform, IT003-000602 (January 2014)

Author

Gilles Ubaghs, Senior Analyst, Financial Services Technology

gilles.ubaghs@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo