Use of artificial intelligence in e-commerce fraud detection and prevention: GDPR risks

Published 30-Mar-2022 by
David Dumont and Anna Pateraki, Hunton

Artificial Intelligence (AI) is increasingly used in financial technology (fintech) solutions. One vital area of AI use in this context is to provide fraud monitoring, detection and prevention services in the context of e-commerce transactions.

These services often analyse various data elements, such as payment data, usage patterns, device information and data enriched from third-party sources. Based on that analysis, the service assigns a certain fraud risk rating for a given transaction that will be used to authorise or decline that transaction, or (depending on the service) require additional verification.

AI technology help train the algorithms that these service use and improve their fraud prevention features on a continuous basis. It is a process that protects consumers from fraudulent transactions, such as those conducted by using stolen credit cards, but requires careful analysis of related data protection issues from a General Data Protection Regulation (GDPR) perspective.

From a contract perspective, the e-commerce site that decides to use a service provider's fraud prevention service often requires that service provider to enter into a data processing agreement. Whether the service provider that provides the fraud prevention service is acting independently as a data controller or on behalf of the e-commerce site as a data processor in practice depends on how the service is set up.

The role of the service provider should be determined at the outset, as this determination will inform the type of contract that the parties should put in place in a specific case (data processor terms vs. data controller terms). In these relationships, it is not uncommon that the fraud prevention service is set up in a way that the service provider is acting as a data controller, although there are cases where the service provider would act as a data processor.

Full spectrum

As a data controller, the fraud prevention service provider would be subject to the full spectrum of data protection obligations under the GDPR, including providing notice about the processing of personal data in its privacy policy and handling data subjects requests about their rights, with or without the cooperation of the e-commerce site (depending on whether the service is based on white label or visible to consumers).

Often, the service provider might act as a data controller where certain conditions are met, including that in order to assign the fraud risk rating, the service (i) combines consumer data from the e-commerce site with huge data sets from different other sources (other e-commerce sites and third-party patterns/analytics), (ii) uses the combined data to provide cross-customer services (use an e-commerce site's data as a basis against which transactions of another e-commerce site would be screened for fraudulent attempts), and (iii) uses the fraud score to approve/reject a transaction in real-time, without involvement/decision from the e-commerce site.

Another factor that may indicate the service provider's qualification as a data controller is that the service needs to use the fraud-related data further for AI training and analysis purposes. The agreement between the parties should clearly anticipate or authorise, where needed, such further processing of personal data for AI-based improvement of the fraud prevention services.

From an accountability perspective, the use of AI to predict the probability of fraud in e-commerce transactions should involve an AI risk assessment. The AI risk assessment is a tool that will help identify and mitigate potential GDPR risks when using such technology.

It should evaluate how the further use of the fraud-related data to train the service provider's algorithm complies with the key principles of the GDPR, such as fair and transparent processing (including ethical use of fraud-prevention models/limiting unwanted bias), purpose limitation and data retention limitations.

In the event that specific privacy and security risks are identified, the assessment should document the relevant remediation steps, such as pseudonymising or encrypting the personal data where technically possible.

Legal basis

Under the GDPR, the processing of personal data requires a legal basis. The consent of the consumer is not always required in the context of fraud prevention activities. The GDPR permits processing of personal data that is strictly necessary for the purposes of preventing fraud under the legitimate interests legal basis of the data controller.

In the context of AI-based fraud prevention services, the assessment mentioned above should, among other issues, clarify the legal basis on which the e-commerce site can rely upon to permit the further use of the data for the purpose of training the service provider's machine learning models to improve the ability to monitor, prevent and detect fraudulent payment transactions.

A specific issue that is often considered is whether the use of AI-based fraud prevention services may lead to automated decision-making (ADM) under Article 22 of the GDPR (which is subject to restrictions). In practice, this issue likely has limited application in the fraud prevention context, as the relevant restrictions apply only where the ADM produces legal or similarly significant effects that are of a negative nature (e.g., deprive a person from legal rights, lead to discrimination or similar serious impactful effects).

In the fraud prevention context, while the assignment of the fraud risk rating can be subject to automatic values (e.g., pre-selected criteria) that would authorise/reject a transaction, or require further verification, such automatic action in many cases would have a more positive effect in protecting the interests of the consumer, that is to protect against fraudulent attempts using valid payment card details. However, a case-by-case analysis is required regarding this issue.

From a governance perspective, the use of AI-based fraud prevention services requires (similar to other AI-based uses) a data protection commitment from the organisation's leadership and oversight functions, close collaboration between cross-functional teams (management, privacy leads, engineers), and internal policies and procedures about the service's compliance with applicable data protection law.

In conclusion, while AI-based fraud prevention technology is a useful tool in preventing harm to consumers, it requires careful consideration from a GDPR perspective.

David Dumont and Anna Pateraki, Hunton

Complaints Procedure