Miles A. Peña

DSC 500 Introduction to Data Science

Matthew Metzger

November 4, 2023

Machine Learning: Fraud Detection

It is reported that approximately one in ten adults falls victim to a scam or fraud every year in the United States. Fraud can affect an individual in many ways often causing trauma and irreversible damage to the one affected as well as their friends and family. Those individuals that fall victim to fraud are not the only ones affected by the crime, however. It can affect governments, businesses, security, and the environment if bad enough. I personally have seen it on multiple occasions at my job where families purchase fraudulent tickets from scammers and are left at the gate embarrassed and ticketless due to fraud.

Machine Learning is one way that we can help with the fraud problem we have in the country. “Machine learning can detect fraud by analyzing huge amounts of raw data under specific instruction to identify patterns and anomalies that indicate suspicious user behavior. It can be human monitored for more accurate results without false positives” (How to Improve Fraud Detection, 2023). Algorithms in machine learning can recognize patterns that deviate from a user’s normal activity. These learn from the data provided by the actual user and flag any suspicious activity that does not fall in line with what the user typically frequents.

Other common applications include risk scoring (which assigns risk scores based on transaction amount, location, and frequency), network analysis (which analyzes relationships between entities in order to identify unusual connections), text analysis (which analyzes things like emails and social media posts in order to identify fraudulent activity), and identification verification (such as biometrics to ensure that a person is who they claim to be). One last application is adaptive learning. “One of the key strengths of machine learning is its ability to learn and adapt to new information. As fraudulent actors change their tactics, machine learning models can be retrained on new data, allowing them to stay up-to-date and better equipped to detect emerging fraud patterns” (How machine learning works, 2023).

Potential drawbacks with using machine learning as a means of fraud prevention lie in the ethics of it all. As with humans, bias can play a part in providing inaccurate information with machine learning. There is also the issue of privacy which is one of the hottest topics with anything data science. I think that this issue specifically will lead to political issues as some will be more okay with feeling their privacy intruded to protect their assets than others creating a divide among the public.

Based on everything provided above, I would still be on the side of using machine learning as a means to prevent fraud. The damage that fraud can cause on individuals, governments, businesses, and the environment is far larger than allowing a machine to learn my patterns to prevent criminals from stealing my information.

References:

How machine learning works for payment fraud detection and prevention. (2023, June 27). *Stripe*. <https://stripe.com/resources/more/how-machine-learning-works-for-payment-fraud-detection-and-prevention>

How to Improve Fraud Detection With Machine Learning. (2023, June 22). *DataDome*. <https://datadome.co/learning-center/fraud-detection-machine-learning/#:~:text=Machine%20learning%20can%20detect%20fraud,accurate%20results%20without%20false%20positives.>

The total impacts of fraud. (n.d.). *Commonwealth Fraud Prevention Centre*. <https://www.counterfraud.gov.au/total-impacts-fraud#:~:text=Human%20impact&text=Fraud%20can%20have%20a%20devastating,opportunities%20for%20individuals%20and%20businesses.>