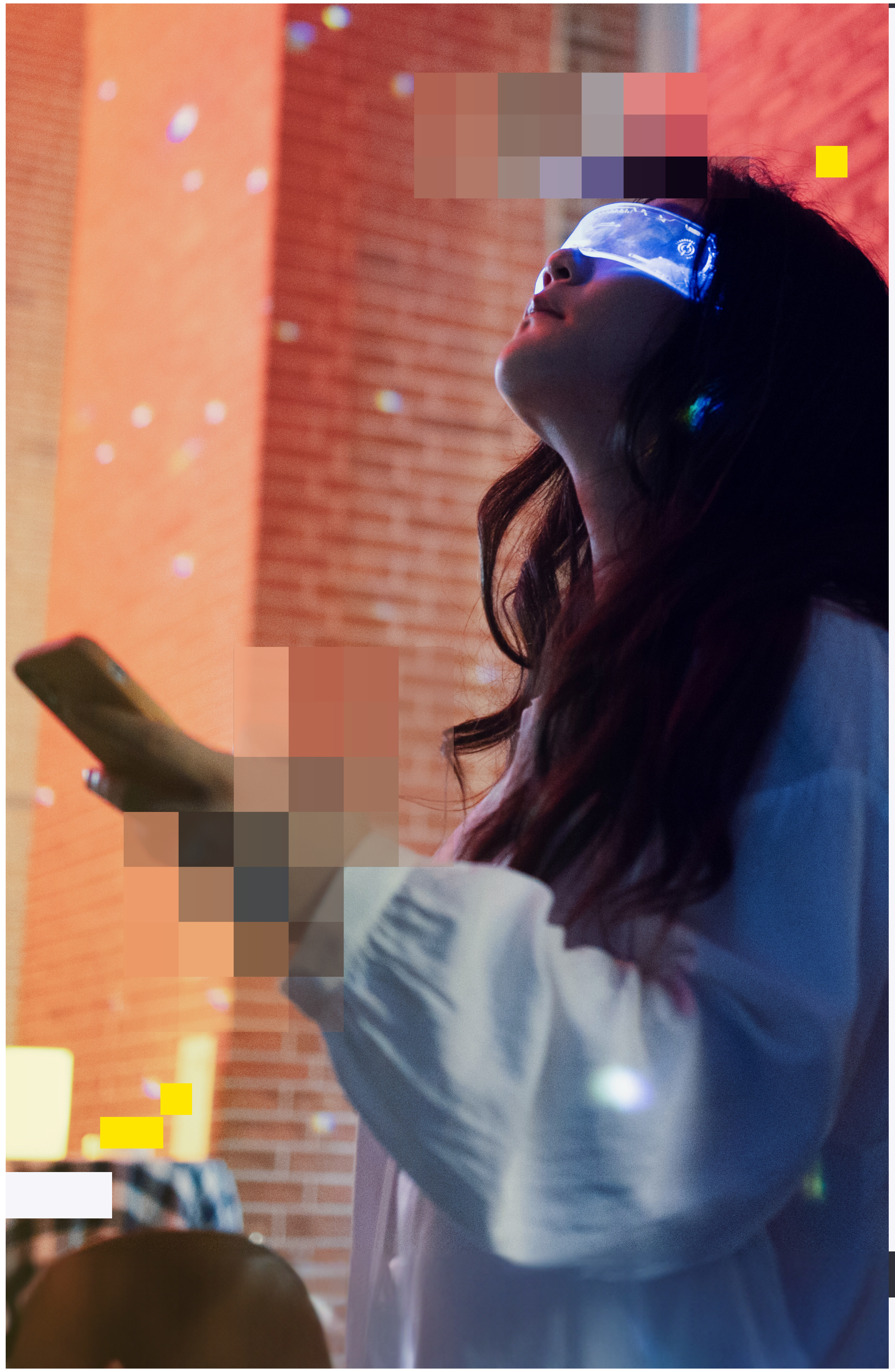
How generative AI can be employed in fraud detection and prevention

April 2024



Introduction

Generative AI (gen AI) is currently one of the most popular topics in business and technology. It's evolving at an incredible speed, leaving us in awe of its potential and capabilities. Its future possibilities seem limitless, sometimes even resembling "mission impossible." We're impressed by its power and speed, and amazed by its creativity and originality. We must also consider its hazards and destructive potential.

When it comes to fraud detection and prevention, genAI serves as a double-edged sword, based on its users' intentions. On one hand, anti-fraud practitioners wield genAI to detect fraudulent activities. On the other hand, criminals are quick to exploit genAI for their fraudulent schemes. Consequently, it becomes an incessant battle.

Let's dive into more details.

How generative AI helps

CREATING SYNTHETIC DATA

One common challenge in dealing with fraud data is imbalance. While machine learning algorithms can address this problem through techniques like oversampling or undersampling with oversampling being more prevalent in fraud detection models, they are unable to generate genuine data. Generative AI, to some extent, tackles this issue by generating synthetic data, albeit with some limitations. This synthetic data can then undergo advanced tuning and anomaly detection, ultimately enhancing the outcomes of the modeling process.

AUGMENTING EXISTING SOLUTIONS

Instead of replacing previous modeling tools and techniques, genAI can enhance and complement existing methodologies by incorporating external data insights and detecting hidden behavioral patterns. Through multiple use cases with EY clients, gen AI has demonstrated its ability to contribute to a robust solution for fraud detection.

DETECTING ID/ SYNTHETIC ID FRAUD

Criminals often use fake IDs to commit fraudulent activities, such as opening new accounts. A notable related example is the increase in fake Canada Emergency Response Benefit (CERB) applications during the pandemic. Traditional AI methods may struggle to detect such sophisticated fraud techniques. However, generative AI's advanced image analytics capabilities offer significant potential in mitigating this issue.

DETECTING DOCUMENT FRAUD

Document fraud has emerged as one of the fastest-growing types of fraud since the pandemic. Criminals use advanced software to create counterfeit documents such as tax forms, banking statements, pay slips and cheques. The battle against document fraud has become a "catch me if you can" scenario, with both criminals and anti-fraud professionals using genAI to gain an edge. Gen AI, with its ability to analyze the metadata of documents, plays a crucial role in detecting fake documents that are often challenging to identify using traditional machine learning algorithms or even human scrutiny.

How generative AI hurts

It's important to acknowledge that gen AI can also be exploited for harmful purposes. Here are a few examples:

VOICE SCAM/VOICE AUTHENTICATION FRAUD

This has become a valid concern, especially as many financial institutions have adopted the human voice as a biometric authentication method. Prior to the advent of generative AI, cloning human voices with accuracy was extremely challenging due to the complexity of vocal characteristics, including tones, pitches, rhythms and emotions. It would have required significant financial resources to create even coarse imitations. However, with Generative AI, this barrier has been overcome. Reports indicate that a US AI lab successfully created a deepfake voice that bypassed a UK bank's security measures after a few attempts. This highlights the emerging threat and the urgent need for banks and other institutions to respond promptly to mitigate the risks associated with voice authentication fraud.

VIDEO SCAM

Criminals can misuse generative AI to create authentic-looking videos by impersonating victims. These malicious actors can then use these videos to deceive others, such as borrowing money from the victim's family and friends or engaging in blackmail.

PHISHING/VISHING

In the past, it was often easier to spot suspicious elements due to criminals' poor craftsmanship. However, with advances in gen AI, criminals can now generate high-quality content that may deceive individuals more effectively. This highlights the evolving landscape of cybercrime, where criminals are using advanced technologies to improve their fraudulent techniques.

SOCIAL MEDIA FRAUD

Criminals can use generative AI to create well-designed and convincing social media profiles for romance scams, and phony company websites for job scams or e-commerce scams. These sophisticated fake profiles and websites can easily deceive individuals.

GenAI and risk

Gen AI has generated significant intrigue and concern among users due to its unrivaled capabilities and inherent risks. Some of the specific concerns include:

RISK OF BIASED OUTPUTS

Generative AI poses a risk of generating biased outputs, which could be even more unpredictable compared to traditional AI methods. The complex nature of gen AI algorithms increases the potential for amplifying existing biases or introducing new ones.

RISK TO DATA PRIVACY

With gen AI potentially having more direct interactions with customers, the risk to data privacy becomes more pertinent. Adequate measures need to be in place to protect sensitive customer information and ensure proper handling of data.

RISK OF MISUSE

This risk of misusing generative AI encompasses issues like misinformation, deepfake manipulation, fraudulent activities and other forms of abuse. It is crucial to establish ethical guidelines and regulations to prevent such misuse.

What can EY Canada's FinCrime team do for you

When implementing generative AI for fraud prevention and detection, we must understand that an effective anti-fraud solution goes beyond technology. It requires an enterprise-wide framework that encompasses various aspects to strengthen the overall fraud prevention ecosystem. Some of these aspects include identity and access management, case management, transaction monitoring, training and education, and reporting and analytics.

AI does not replace professionals but rather complements their expertise. We acknowledge this and offer services to conduct comprehensive risk assessments for clients. These assessments help identify any gaps or vulnerabilities in your risk management processes and controls.

EY Canada's FinCrime team is well-equipped to help organizations of varying sizes across a variety of industries address fraud risks. With deep knowledge and extensive network, our team can provide customized solutions to effectively tackle your unique fraud challenges.

Contact us

RAMZI BOU HAMDAN

Partner

FinCrime/AML Advisory Practice Lead
Risk Consulting, EY Canada
ramzi.bouhamdan@ca.ey.com

YARA ELIAS, PH.D.

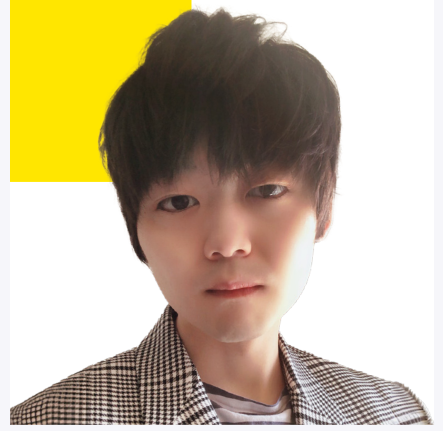
Senior Manager

AI Risk, Risk Consulting
EY Canada
yara.elias@ca.ey.com

SAURABH MADAN

Manager

Fraud Risk, Risk Consulting
EY Canada
saurabh.madan@ca.ey.com



DENNIS ZHAO

Senior Consultant

Fraud Risk, Risk Consulting
EY Canada
dennis.zhao@ca.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

4516979

This publication contains information in summary form, current as of the date of publication, and is intended for general guidance only. It should not be regarded as comprehensive or a substitute for professional advice. Before taking any particular course of action, contact Ernst & Young or another professional advisor to discuss these matters in the context of your particular circumstances. We accept no responsibility for any loss or damage occasioned by your reliance on information contained in this publication.

ey.com/ca