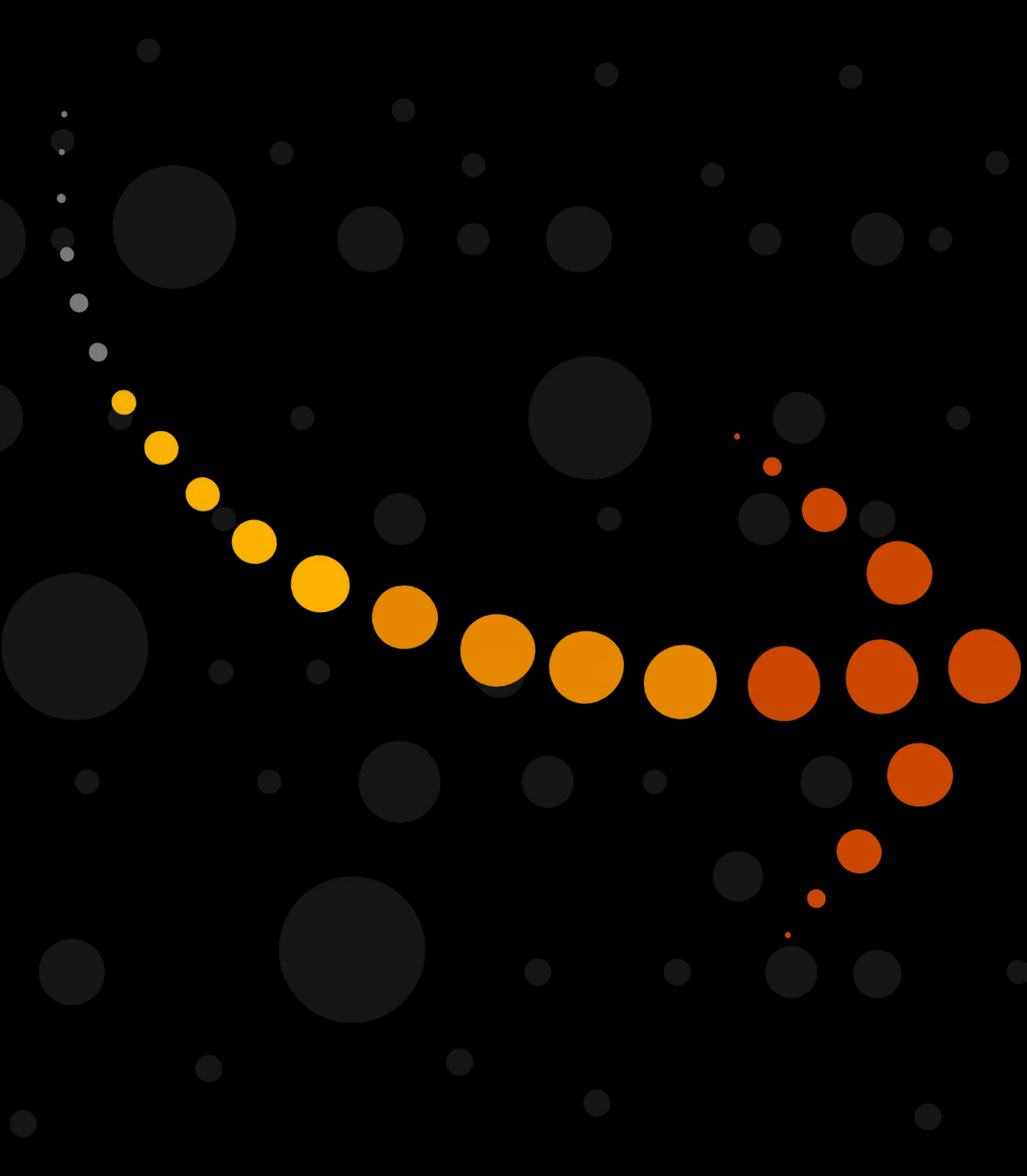
pwc

Leveraging GenAI in banking:

Opportunities, risks, and security measures

Table of **contents**



01

Introduction

Introduction

In a dynamic banking environment, banks are seeking to differentiate themselves and gain a competitive advantage. Generative Artificial Intelligence (GenAI) is transforming the banking sector, providing innovative solutions that optimise efficiency, enhance security, and increase customer satisfaction.

As the banking industry increasingly moves towards digitisation, the adoption of advanced AI technologies becomes crucial. GenAI, with its ability to synthesise and generate content, offers unparalleled opportunities to automate complex processes, provide personalised customer experiences, and strengthen security measures.

Our latest 27th Annual CEO Survey indicated that leaders expect technology including GenAI and Machine Learning (ML) to be the centre of optimising costs, creating new revenue streams and improving the customer experience within their organisations. Middle East CEOs are also optimistic about the financial impact of GenAI, with 63% expecting the adoption of it in their organisation to increase revenue, while 62% said it would increase profitability. In the GCC, enthusiasm is even higher with two thirds expecting revenue increases and a similar number expecting profitability increases. While these statistics cover various industries, the banking sector specifically has been heavily reliant on technology since its inception.

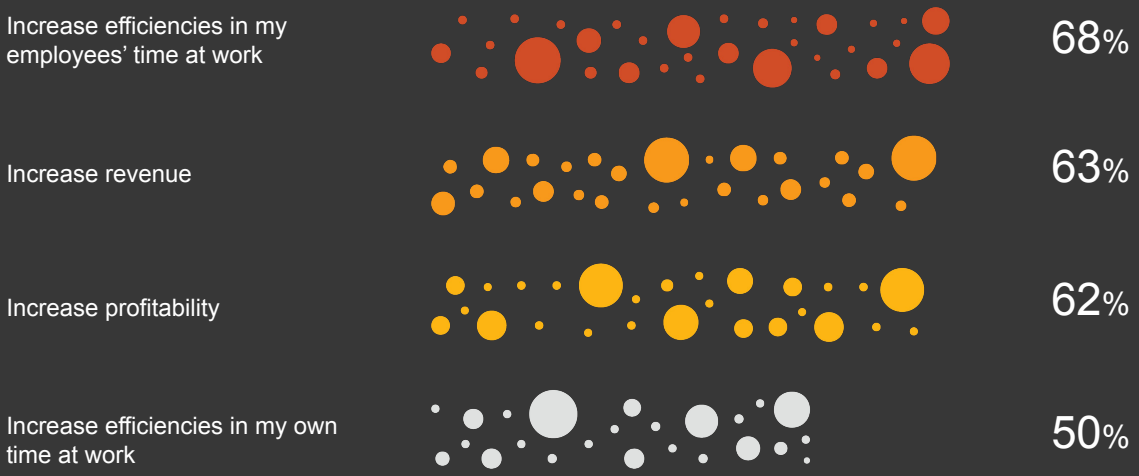
Financial services CEOs in the region have acknowledged the necessity to evolve their business models to ensure sustainable outcomes for stakeholders and society, especially in the face of challenges, such as climate change and the rise of GenAI.

Findings of our 27th Annual CEO Survey: Financial Services findings have indicated that almost three-quarters of FS CEOs in the region (75%) expect GenAI to improve the quality of their products and services over the next year, significantly higher than 59% of global FS peers. An equally significant number of FS leaders in the region (69%) believe that GenAI will enhance their company's ability to build trust with stakeholders, compared to less than half of their global peers (47%).

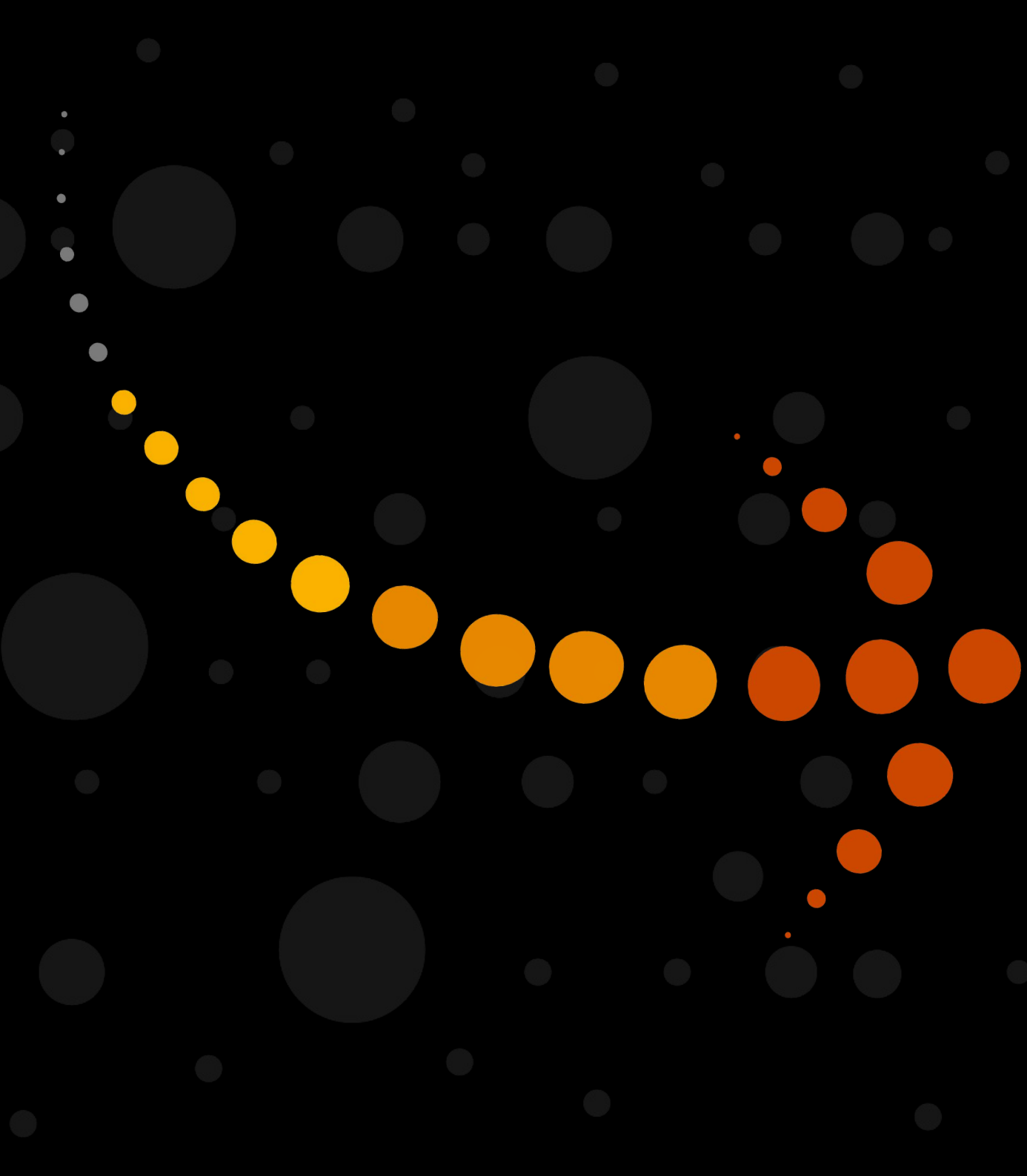
AI systems can generate content, predict outcomes, automate complex processes, and much more, potentially transforming how banks operate, engage with customers, and manage data. However, alongside these benefits come substantial cybersecurity risks that must be managed to protect sensitive financial information and maintain trust in banking institutions.

In this thought leadership report we will dive into the use cases of GenAI in banking, identify associated cybersecurity risks, and recommend measures to mitigate these risks.

How will GenAI affect your company this year?



Q: To what extent will GenAI increase or decrease the following in your company in the next 12 months? (Showing summary 'NET' Increase)
Source: PwC's 27th Annual CEO Survey, base of 4,702, US base of 231



02

Personalisation and security: Use cases of GenAI in banking

Personalisation and security: Use cases of GenAI in banking

GenAI is revolutionising the banking industry by enhancing operational efficiency and customer satisfaction. As the market moves toward cashless banking, GenAI introduces a unique opportunity for banks to explore untapped possibilities and overcome existing limitations.

Leveraging GenAI can enable banks to create personalised experiences for each customer while maintaining robust security systems. This tailored approach addresses logical hazards and minimises complications arising from traditional practices. In a competitive landscape, banks are constantly seeking to reduce costs, pioneer new products and services that gain customer support, and advance their market share.

Adopting GenAI will help banks realise these objectives through various use cases. In this section we touch base on these scenarios, their benefits and primary risks.

Streamlined loan and mortgage processing

GenAI can lower the threat assessment and scoring within the loan approval or mortgage eligibility process and dramatically lessen time to final approval – from weeks to days to even hours at times. Sophisticated AI models can make more precise decisions and lower the probability of defaults by assessing risks such as credit scores, incomes, work experience, and liabilities.

Using an Optical Character Recognition (OCR) system, GenAI can automate the process of pulling in pay stubs and tax returns to extract and validate this data, allowing the process to run faster and with significantly lower risk of human error.

GenAI algorithms can be updated based on the applicable regulations and legality of data processing.

The model can also help with proactive credit risk management and loan portfolio optimisation via predictive analytics to forecast likely defaults and classify accounts at risk.

GenAI automates repetitive tasks, reducing operational costs and allowing banks to direct funds to strategic areas as well as customer relationship management.

The integration of GenAI in loan and mortgage processing delivers great efficiencies; however, it also exposes a cluster of risks that need to be cautiously managed:

Data privacy

Customer interactions with AI systems involve sharing sensitive personal and private information, either provided by the customers or recorded within the massive dataset utilised by GenAI. Such data can be exposed through a cyber breach or via AI gaslighting – which occurs when GenAI applications provide information that is misleading or biased – ultimately leading to data compromise.

Lack of clarity and transparency

Loan and mortgage processing AI models generally work like "black boxes", meaning it is difficult to interpret how a decision is derived based on given data. The lack of explanation and transparency can be harmful because you would not be able to trust the results and verify the possible errors or biases in the process of taking the decision.

Bias and discrimination

Learning from historical data, GenAI algorithms may grasp current biases and discriminatory practices. If not properly dealt with and minimised, this bias could cascade through the automated decision-making process in loan and mortgage processing, potentially reinforcing or exaggerating current biases, leading to unjust or discriminatory outcomes towards various groups of applicants.

Service disruption

GenAI systems require robust infrastructure, network connectivity, and reliable data sources to function effectively. Any disruptions or technical failures in these areas can impact loan and mortgage processing, leading to delays, errors, or system downtime that can negatively affect customer experience and business operations.

Non-compliance

Failure to regularly update the GenAI model with newly introduced laws and regulations may lead to risk of noncompliance and, ultimately, regulatory or financial penalties.

Streamlined loan and mortgage processing

GenAI can lower the threat assessment and scoring within the loan approval or mortgage eligibility process and dramatically lessen time to final approval – from weeks to days to even hours at times. Sophisticated AI models can make more precise decisions and lower the probability of defaults by assessing risks such as credit scores, incomes, work experience, and liabilities.

Using an Optical Character Recognition (OCR) system, GenAI can automate the process of pulling in pay stubs and tax returns to extract and validate this data, allowing the process to run faster and with significantly lower risk of human error.

GenAI algorithms can be updated based on the applicable regulations and legality of data processing.

The model can also help with proactive credit risk management and loan portfolio optimisation via predictive analytics to forecast likely defaults and classify accounts at risk.

GenAI automates repetitive tasks, reducing operational costs and allowing banks to direct funds to strategic areas as well as customer relationship management.

Streamlined loan and mortgage processing

The integration of GenAI in loan and mortgage processing delivers great efficiencies; however, it also exposes a cluster of risks that need to be cautiously managed:

Data privacy

Customer interactions with AI systems involve sharing sensitive personal and private information, either provided by the customers or recorded within the massive dataset utilised by GenAI. Such data can be exposed through a cyber breach or via AI gaslighting – which occurs when GenAI applications provide information that is misleading or biased – ultimately leading to data compromise.

Lack of clarity and transparency

Loan and mortgage processing AI models generally work like "black boxes", meaning it is difficult to interpret how a decision is derived based on given data. The lack of explanation and transparency can be harmful because you would not be able to trust the results and verify the possible errors or biases in the process of taking the decision.

Bias and discrimination

Learning from historical data, GenAI algorithms may grasp current biases and discriminatory practices. If not properly dealt with and minimised, this bias could cascade through the automated decision-making process in loan and mortgage processing, potentially reinforcing or exaggerating current biases, leading to unjust or discriminatory outcomes towards various groups of applicants.

Service disruption

GenAI systems require robust infrastructure, network connectivity, and reliable data sources to function effectively. Any disruptions or technical failures in these areas can impact loan and mortgage processing, leading to delays, errors, or system downtime that can negatively affect customer experience and business operations.

Non-compliance

Failure to regularly update the GenAI model with newly introduced laws and regulations may lead to risk of noncompliance and, ultimately, regulatory or financial penalties.

Enhanced cybersecurity

GenAI can enhance cybersecurity practices such as real-time threat detection and response. It continuously monitors logs and traffic, user patterns, and system operations, making use of advanced ML algorithms and data analytics.

An important capability of GenAI is that it learns, and it does this live in order to stay ahead of evolving cyber risks and safeguard sensitive financial data. One such example is the ability to detect insider threats by analysing anomalies in employee behaviour that may betray malicious intent or compromised credentials.

GenAI's ability to automate quarantining affected systems, blacklist IP addresses, and send alerts to security teams can help reduce the impact of cyber attacks, curtailing the severity of harm and downtime.

Additionally, GenAI bolsters the security profile of banks as a whole by training threat-detection models through tens of thousands of samples in ML methods. This continual enhancement aims to help banks become more resilient in the face of new and evolving threats, reinforcing their ability to prevent cyber attacks. – enabling financial organisations to boast a higher level of security, secure vital assets, and, most importantly, maintain customer trust.

While there are an enormous amount of positives to integrating GenAI into cybersecurity frameworks, doing so also comes with a new set of risks:

False positives and false negatives

GenAI-based threat detection systems may generate false positives, flagging legitimate activities as potential threats and overwhelming security teams with a high volume of false alarms, or false negatives, which fail to detect actual threats and may leave the organisation vulnerable to attacks.

Adversarial attacks

Malicious actors may attempt to deceive GenAI threat detection models by crafting inputs specifically designed to evade detection or trigger false alarms. Such adversarial attacks can undermine the effectiveness and reliability of the threat detection system, with successful attacks potentially going unnoticed.

Data leakage

Real-time threat detection relies on analysing a significant amount of sensitive data, such as network traffic logs or user behaviour patterns. Inadequate security controls could expose sensitive information and compromise the security of the bank.

Precise identity verification

Biometric authentication

Biometric authentication has the potential to dramatically streamline the identity verification onboarding process. GenAI can play a foundational role here, with advanced facial recognition complemented by voice recognition systems that can quickly and precisely identify a customer.

Customers can be prompted to upload a selfie and a voice recording through their banking app or at an ATM to access services. These biometric data points are matched against the photos and voice samples present on the customer's supplied IDs using high-level AI-based algorithms. This not only adds robustness to security but also provides customers with a seamless experience.

Biometric authentication helps eliminate dependence on legacy password-based systems that are more vulnerable to breaches and attacks logging elevates the risk factors. Furthermore, it helps prevent identity theft and fraud by assessing whether the person attempting to avail services is who they claim to be. In addition, its integration into biometric systems ensures self-learning and continuous improvement, which increases accuracy and reliability in verifying human identities over time.

Deepfake detection

In response to the increasing danger of new information hazards, modern manipulative content is scrutinised by advanced GenAI models, which determine whether we are facing synthetic identities or fake-manoeuvring. These models are able to detect imperceptible indications of fraud, such as small procedural discrepancies in facial expressions or audio artefacts that are difficult for the human eye or ear to detect. GenAI is more capable of recognising deepfake signs, making the verification process more secure to keep banks secure from the threat of forgeries.

Due to this, GenAI-driven platforms that can identify deepfakes are invaluable for security practices such as Know Your Customer (KYC) checks and to help meet regulatory compliance. This improves operational efficiencies by streamlining the validation process and reducing the margin for errors. GenAI-backed KYC processes also increase customer confidence in the guarantee of identity protection.

Precise identity verification

As beneficial as GenAI may be, it also poses risks that must be examined:

False positives and false negatives

GenAI-based identity verification systems may generate false positives, wrongly flagging and denying access to legitimate individuals as potential risks, or false negatives, failing to detect fraudulent or unauthorised activities, potentially leading to financial losses or reputational damage.

Trust and customer experience

Over-reliance on GenAI for identity verification may undermine customer trust if the system generates too many false positives or imposes burdensome verification processes. Balancing security with a seamless, user-friendly experience is crucial to maintain customer satisfaction.

Bias and discrimination

GenAI algorithms can inherit biases present in training data or algorithm design, which can lead to discriminatory outcomes, such as incorrectly identifying certain individuals or groups as high risk based on biased patterns. This can result in unfair treatment, potential legal issues, and damage to the organisation's reputation.

Service disruption

Enhanced identity verification processes often involve the collection and analysis of sensitive personal data. It is crucial to ensure robust data privacy and security measures to protect this data from unauthorised access, breaches, or misuse. Inadequate security controls could expose personal information and compromise individual privacy rights.

Automated customer support and personalised banking services

GenAI can power sophisticated chatbots and virtual assistants capable of handling a wide range of customer inquiries, from account balance queries to complex transaction issues. These AI-driven tools are designed to provide instant, accurate responses to customer questions, significantly improving the efficiency and quality of support services. By leveraging natural language processing and ML, these virtual assistants can understand and interpret customer queries, offering personalised, contextually relevant solutions. They can also learn from interactions, improving their response accuracy and expanding their knowledge base over time. This automation frees up human customer service representatives to focus on more complex, higher-value tasks. Additionally, GenAI-powered chatbots can operate 24/7, which is particularly beneficial in a global banking environment where customers may be located in different time zones. By integrating GenAI into customer support, banks can achieve a higher level of service excellence, reduce operational costs, and streamline support processes, enabling a more robust, customer-centric banking experience.

While there are many benefits, integrating GenAI into customer support systems involves some risks as well:

Data privacy

Customer interactions with AI systems involve sharing sensitive personal and private information, either by the customers or recorded within the massive dataset utilised by GenAI. Such data could be exposed and/or compromised through a cyber breach or via AI Gaslighting.

Misinformation

Without comprehensive testing of scenarios, and with GenAI able to learn from conversations between customers, GenAI may overwrite data, leading to the provision of inaccurate or incomplete information due to errors or manipulation.

Bias

GenAI relies on complex AI algorithms and scenarios. The model is usually trained on a specific dataset, which may neglect differences in customers' cultures, leading to the presence of biased responses and/or discriminatory customer interactions.

Service disruption

Customer support is one of the most critical services in the banking sector. Disruption in service due to cyberattacks or unavailability of the GenAI model may lead to customer dissatisfaction and reputational impacts.

Automated customer support and personalised banking services

The banking industry is rapidly changing, and GenAI has been a big part of this change, using AI to analyse customer data to provide custom product recommendations and financial advice based on each customer's profile. By evaluating transaction history, spending type, and financial targets, banks can present tailor-made experiences that fit the special requirements and tastes of each customer. This is complemented by a level of personalisation not present in other traditional solutions, made possible by GenAI providing automated investment advice and wealth management services with strategies adapted dynamically to real-time market data, a customer's financial conditions, and individual risk profiles. These custom services increase customer satisfaction by enabling them to make better financial choices, build smarter investment portfolios, and reach their financial targets faster. GenAI integration empowers banks to deliver a frictionless, hyper-personalised experience, enhancing customer loyalty and the bank's competitiveness.

While there are multiple advantages, incorporating GenAI into personal banking services also brings risks:

Inaccuracy or malfunctions

GenAI uses massive datasets; a lack of data pertaining to one or more customers may lead to inaccurate personalised banking services.

Bias and fairness

GenAI uses massive datasets; a lack of data pertaining to one or more customers may lead to inaccurate personalised banking services.

Data security

Collecting and processing extensive customer data increases the risk of data breaches.

Compliance

Banks must ensure that the use of GenAI in handling customer data complies with internal policies and all relevant data protection laws and regulations in their region, such as GDPR in Europe.

Fraud detection and prevention

Fraud detection is another vital area that GenAI can handle very well. In transaction patterns, AI models can monitor and identify which transactions present anomalies. These models use a combination of supervised and unsupervised learning to spot peculiar behaviour – for example, if a customer suddenly withdraws a lot of money, is making multiple transactions in a short time, or chooses different times to do business from new places. When tens of terabytes of data being analysed in real time, instantaneous alarms of suspicious activity can be given both to the bank and to customers. This enables banks to be proactive, taking the needed actions before a fraud incident can even succeed.

Besides real-time detection, GenAI enhances continuous monitoring and risk assessment. GenAI keeps evolving by learning from past instances and adjusting its detection algorithms accordingly, ensuring that banks are always ready to meet any imminent threat. Such a proactive approach means that banks will not only be able to respond to incidents better but are able to anticipate fraud risks before they escalate. GenAI-powered fraud detection systems also improve the accuracy of risk assessment by taking into account a wider range of factors and variables, which traditional methods typically ignore. These include customer behaviour, transaction history, device information, and geolocation data.

This wealth of information enables GenAI to provide a better-rounded judgement on fraud risks than any one source alone could furnish. GenAI systems can also perform risk scoring and arrangement in a more strategic way than human analysts, ensuring the most important threats are addressed first. All this cuts down on document-handling drudgery for people, freeing them up to concentrate on crucial cases and guiding to a better, more agile overall strategy. As a result, overall security is improved significantly, customer trust and satisfaction are safeguarded, and fraud can be better averted.

GenAI has the ability to generate a mass of artificial data that emulates real transaction data. It is also a major stepping stone towards stronger fraud detection models, given the vast number of trials that emerge from this work.

Such tools are particularly useful in situations where government or other regulations prevent the use of real customer data.

This allows for broader, richer data sets, significantly enhancing the accuracy of fraud detection models without compromising user privacy.

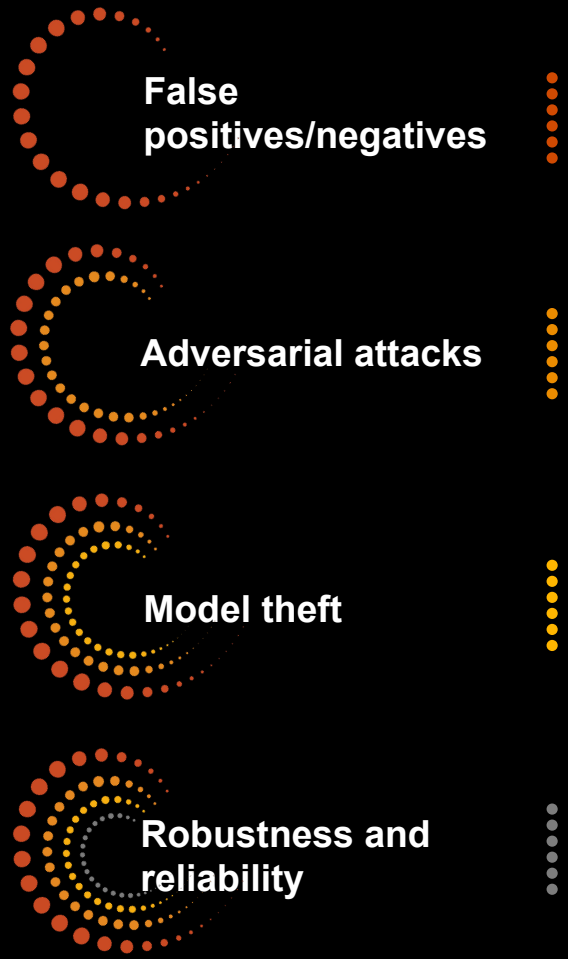
It can improve the ability to understand and recognise complex patterns and anomalies within data through the superior design of models purpose-built with this in mind.

These algorithms can simulate a wide range of fraudulent behaviours, which will improve existing systems for sensing dangerous signals from both advanced and novel fraud schemes.

Fraud detection and prevention

Real-time decision-making can be achieved by incorporating GenAI into transaction systems. Instant analysis models of GenAI examine the context of every transaction ‘live’ and compare it to historical data. They can spot any deviations immediately for subsequent action, which reduces the delay between fraud detection and capture, providing the ability to block or flag suspicious transactions in their early stages.

While such benefits may come with adopting GenAI in fraud detection systems, there are several risks that one should be aware of (and mitigate). Given AI involves so many moving parts, there are key risk factors inherent to the different levels of complexities and the continuous process of incorporating new tactics that fraudsters adopt. In addition, financial data is sensitive information and maintaining consumer confidence is critical. The risks posed by these threats are pronounced, requiring stronger protections and ongoing monitoring.



False positives/negatives

GenAI may flag legitimate transactions as fraudulent or fail to detect an actual fraudulent transaction. This misidentification can either lead to unnecessary customer inconvenience and erode trust, or overlooked fraud and financial losses.

Adversarial attacks

Fraudsters may use sophisticated techniques to fool AI models into misclassifying fraudulent transactions as legitimate.

Model theft

Cyber attackers might steal proprietary AI technology or manipulate AI algorithms, leading to significant malfunctioning, poor detection, security issues, and competitive risks. Protecting these models from theft or unauthorised replication is a significant concern.

Robustness and reliability

The robustness of AI models against evolving cyber threats is a constant challenge. Ensuring that AI systems can perform reliably under malicious attacks or when confronted with deceptive information is critical.

Risk Management

Risk management as a key function in the banking sector is a powerful place for the implementation of GenAI. The technology allows banks to simulate hundreds of different economic and financial scenarios in order to forecast future risks and corresponding outcomes, helping to identify potential risks linked to market variability, economic slowdown, and other uncertain financial conditions.

GenAI tackles this issue by crunching huge volumes of data from hundreds of years of experience in real time, building predictive models that guide banks to stay ahead while minimising risk on loans, credits, and investments. This helps banks make more educated decisions, in turn decreasing the likelihood of defaults and financial losses.

One powerful use case for GenAI here is to predict and assess the ability of an applicant to repay their loan under different scenarios, based on their financial history, contemporary economic indicators, and other factors. Likewise, within investment decisions, GenAI can help banks model the effects of different economic conditions on their investment portfolios so they can adjust their strategies for maximum returns and minimum risk. With this, banks can integrate GenAI (or its underlying technology chain) into their risk management frameworks and adopt a more automated and analytical approach towards financial risk management, which can improve the resilience and profitability of a bank.

Although there are numerous benefits of integrating GenAI into risk management systems, it comes with certain risks:

Error propagation

Errors can spread and amplify through a bank's risk management system. This can lead to incorrect assessments of financial products or market conditions, potentially resulting in poor strategic decisions.

Model opacity (Black Box issue)

GenAI models, particularly those based on deep learning, can be highly opaque, meaning it's difficult to understand how they arrive at certain conclusions or predictions. This lack of transparency can be problematic in risk management, where banks need to be able to explain and justify their decisions to regulators and stakeholders.

Dependency and systemic risk

Over-reliance on AI for risk assessments can lead to systemic risks. If many banks are using similar AI models, they might all be exposed to the same types of errors or failures, potentially leading to a systemic crisis.

03

Recommendations to mitigate risks

Recommendations to mitigate risks

While GenAI offers several advantages for the banking and FinTech market, it also introduces risks that need to be effectively mitigated, which may have important implications for financial institutions. These steps should be taken in advance to ensure the integration of GenAI is advantageous:

1. **Implement robust data governance**
2. **Enhance AI system security**
3. **Monitor AI systems Continuously**
4. **Comprehensive testing**
5. **Adhere to NIST AI risk management framework**
6. **Build a customized GenAI strategy**

Implement robust data governance

Banks must ensure that data used by AI systems is accurate, adequately anonymised, and securely stored. Strong data governance can be implemented through but not limited to the following:

- Clear data handling policies and procedures to provide a unified experience for employees with access to the AI's data.
- Establishing strict access controls and regular audits can prevent unauthorised data access and leakage.
- Strong encryption protocols that safeguard data at rest and are transmitted throughout the GenAI.
- Secure storage mechanisms to ensure that vectors or data storages are protected against unauthorised access or manipulation.

Enhance AI system security

Use secure coding practices to protect source code from bugs, errors, and backdoors. Your developers must adhere to secure coding protocols, have peer reviews for every piece of code they build, along with the usage of automated tools that will scan the code to propose the most common bugs on the earlier stage in the software development lifecycle they have been coded. AI systems must be constantly updated and patched against known vulnerabilities. This involves keeping all components of the AI system – including libraries, frameworks, and dependencies – updated with the latest security patches and updates. Establishing a robust patch management process ensures timely application of updates and reduces the risk of exploitation.

Monitor AI systems continuously

Ongoing monitoring to detect and respond to potential security threats is necessary. Additionally, key performance and risk indicators pertaining to the GenAI model should be identified, documented, and monitored, where any deviation should be reported to top management in a timely manner in order to proactively mitigate any potential inefficiency or risks. Implementing real-time monitoring tools to track AI system performance and integrating these with existing Security Information and Event Management (SIEM) systems offers enhanced threat detection. Develop a response plan outlining steps for investigation, containment, remediation, and recovery, along with recommended actions for mitigation. Keeping top management informed ensures prompt and informed decision-making.

Comprehensive testing

Comprehensive testing through adequate use cases and data is vital to help ensure that the GenAI module is reliable and secure. Such testing should include assessing potential bias and discrimination, data integrity issues, and AI Gaslighting scenarios. Simulation of potential attack scenarios on AI systems through regular penetration tests and red teaming exercises can identify and address vulnerabilities before they can be exploited.

Upon development of test cases and scenarios, the relevant team should identify limits to measure the trustworthiness of the technology. Testing trustworthiness should be conducted on a periodic basis, with results reported to senior management and any deviation from desired values remediated. Continuous testing against new adversarial techniques and refining models accordingly is essential to maintaining their robustness.

Adhere to NIST AI Risk Management Framework

Adhering to the NIST AI Risk Management Framework, banks should assess AI technology risks and implement strategies that align with their cybersecurity posture. This includes defining governance structures, forming committees with stakeholders, and developing policies addressing data privacy, security, ethics, and compliance. Continuous oversight through regular audits and third-party reviews is essential. Banks need to establish comprehensive policies and procedures for data management, model development, testing, deployment, and incident response, including AI-specific plans.

Roles and responsibilities need to be clearly defined, with regular training on GenAI risks and management provided. Thorough risk assessments to set risk tolerance levels aligned with the overall strategy are a must, while robust GenAI models can be maintained by following best practices, ensuring security against attacks, and continuously monitoring performance and risks. Finally, banks should regularly evaluate and update AI models, considering new threats and regulatory changes, and establish feedback mechanisms for ongoing improvement. By following these steps, banks can effectively mitigate GenAI risks, ensuring secure and responsible AI use.

Build a customised GenAI strategy

Organisations need to prepare for the GenAI era by establishing customised strategies to become GenAI-ready and have a structured transformation programme. This will require proper integration and alignment with existing business, digital transformation, and cybersecurity strategies to avoid inconsistent use cases or GenAI solutions, bring the utmost value to the business, avoid operational disruption, and minimise risk.

04

GenAI: a game changer for banking

GenAI: Balancing innovation, security, and customer-centricity

GenAI offers tremendous potential for enhancing efficiency, personalisation, and customer engagement in the banking sector. However, it also introduces new cybersecurity risks that must be carefully managed. To mitigate these risks, banks need to implement additional security measures, particularly in securing data, ensuring its accuracy and completeness, and maintaining service availability.

Unlocking customer behaviour and market insights

Additionally, the improved data analysis potential of GenAI allows banks better understanding of customer behaviour and market trends, unlocking hyper-personalised financial products and services and, ultimately, stronger customer relationships and loyalty. GenAI predictive insights enables early tracking of market changes, providing advance warning to banks over changes they can leverage before competitors discover emerging opportunities.

Enhancing cybersecurity with GenAI

Also notable are the cybersecurity improvements GenAI is driving. With cyber threats maturing by the day, the ability of GenAI to detect and react almost instantly to these threats is priceless. As well as keeping valuable financial data safe, this will also help establish trust with customers who need to know that their information is in safe hands.

Integration with emerging technologies

Through incremental development, the evolution of GenAI will pave the way for the most sophisticated applications in the banking sector. Integration with compatible up-and-coming technologies such as blockchain and Internet of Things (IoT) offers the potential to further expand the capabilities and benefits of GenAI. The banks that adopt these innovations will be best poised to take the lead in digital transformation and establish new benchmarks in efficiency, security, and customer experience for the industry.

Strategic partnerships and responsible innovation

Considering the pace at which emerging technologies and GenAI are expanding, banks should consider having the right partners and alliances that can support the implementation of GenAI within their environment while mitigating the risks arising from adopting such technologies.

Making financial services more secure, efficient, and customer-centric

Ultimately, the goal is to harness the power of GenAI responsibly, ensuring that innovation does not come at the cost of security and customer trust. By implementing mitigation strategies, financial organisations can balance leveraging the benefits of GenAI and maintaining robust cybersecurity measures. This approach will help safeguard customer data, maintain trust, and drive sustainable innovation in the digital banking landscape.

GenAI is a gamechanger for banking. It will significantly help make the overall financial services process more secure, efficient, and customer-friendly. As banks continue on this journey, they can look forward to a more innovative and resilient future, with GenAI as a core component of their digital strategy. This ongoing commitment to innovation will be crucial for staying ahead of the competition and meeting the evolving needs of clients in a digital-first world.

Contributors

Fady Chalhoub

Cybersecurity and Digital Trust Partner

Samer Omar

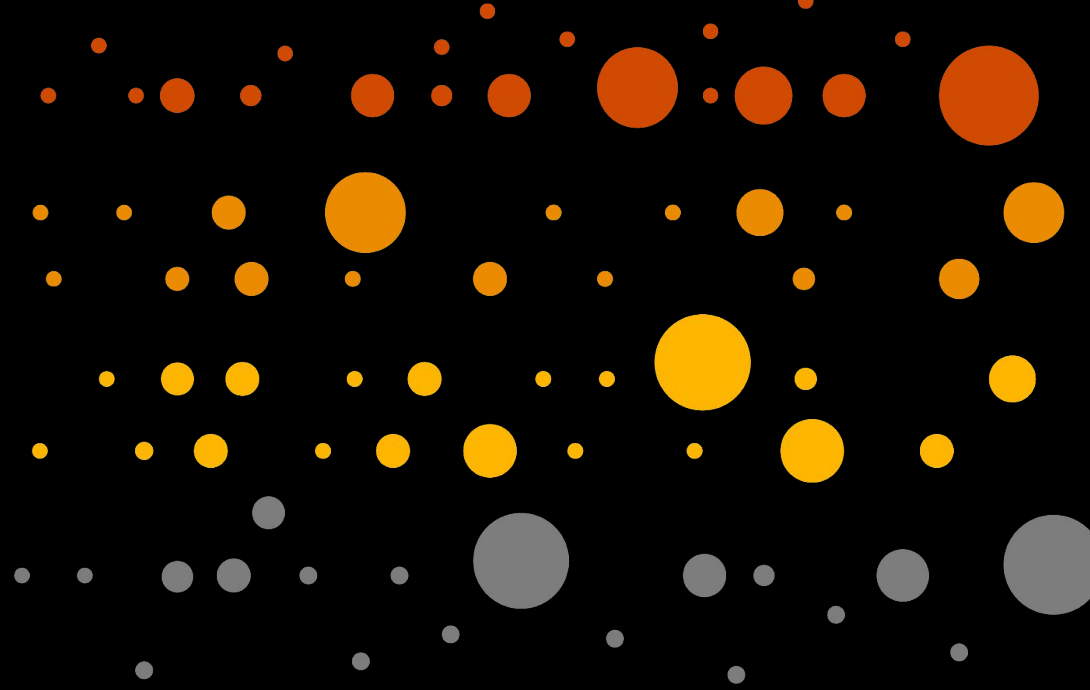
Cybersecurity and Digital Trust Leader

Eyad Haddad

Cybersecurity and Digital Trust Senior Manager

Yasmeen Abdullah

Cybersecurity and Digital Trust Manager



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with nearly 364,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for over 40 years, PwC Middle East has 30 offices across 12 countries in the region with around 11,000 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.