

Guarding the gateway

Combatting real-time fraud in
card-not-present transactions



Capgemini 

 MongoDB®

The many faces of payment fraud

Fraud in payments has many faces and has become increasingly vast. Whether it's an acquiring bank, a card network or scheme, or a card issuer, everyone shares a common goal: to minimize fraudulent activity in payment transactions, thereby preventing financial losses, improving customer satisfaction, and enhancing retention. However, as payment systems have become more sophisticated, so have the fraudsters' methods. They have evolved, employing increasingly complex tactics to steal personal information, clone card details, and ultimately siphon off money.

Today, the threat of payment fraud looms larger than ever, as cybercriminals relentlessly innovate and adapt to bypass security measures. In fact, global card losses due to fraud are projected to total an astounding \$397 billion during the next ten years, including \$165 billion in the United States alone.¹ While there are many factors driving these results, the root cause often lies in the fragmented IT landscapes of financial institutions. Despite housing vast databases rich with multiple data entities, many systems fail to focus on crucial data attributes such as merchant category codes, countries of transactions, cardholder details, or transaction amounts. As a result, fraudulent transactions find their way through the cracks, undetected until it's too late.

Global card losses due to fraud are projected to total an astounding
\$397 billion during the next ten years

The most common types of fraud within payments include:

- ➔ **Merchant fraud**
Someone poses as a legitimate business to deceive the customers and commit financial fraud.
- ➔ **Phishing**
Social engineering attacks through psychological manipulation using fraudulent emails or messages.
- ➔ **Skimming**
Sophisticated devices are often used at ATMs or point of sale (POS) terminals to collect card data.
- ➔ **Identity theft**
Personal identifiable information (PII) is stolen to open bank accounts to initiate fraudulent transactions.
- ➔ **Chargeback fraud**
Raising disputes on legitimate transactions to get the debit amount reversed.
- ➔ **Card-not-present fraud**
Unauthorized card purchases by stealing card information and using it online.

In the US, the categorization of fraud is outlined by the Office of the Comptroller of the Currency (OCC) and is largely followed by most financial institutions.²

1. <https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675/>

2. <https://www.occ.treas.gov/news-issuances/bulletins/2019/bulletin-2019-37.html>

The rising threat of card-not-present fraud

Card-not-present (CNP) fraud is currently one of the most significant challenges facing the payments industry. According to a recent report, merchants lost \$38 billion in 2023 due to online payment fraud, with a projected increase to \$91 billion by 2028.³ The main difference between card-not-present fraud and card-present fraud is the nature of the transaction and the level of risk associated with each type of fraud. In CNP transactions, the card details are stolen as opposed to the physical card itself in a card-present transaction. CNP transactions are

therefore riskier, and fraud detection is even trickier due to the lack of a physical card, chip, PIN, or signature verification.

With CNP transaction fraud, the liability primarily lies with the merchant until a chargeback raised on the transaction proves it differently. While 3D Secure protocols and two-factor authentication add an extra layer of security, it is critical to implement a fraud detection approach that can be integrated both at the acquiring and issuing side of the transaction.



Addressing the gaps in current fraud detection approaches

Current fraud detection approaches used by many payment service providers focus on legacy methods for processing transactions. As a result, they often fail to fully capitalize on the benefits of switching to ISO 20022, increasing data entities, and using artificial intelligence (AI) and machine learning (ML) algorithms to enhance accuracy, speed, and reduce false positives.

Typical gaps in current fraud detection approaches include:



More data than ever before

The payments industry has transformed from handwritten ledgers to modern businesses managing both physical and online sales. This surge in data volume complicates the detection of first-, third-, and fourth-party fraud which have increased in recent years. Sophisticated data and technology solutions are required for effective fraud prevention and detection.



Balancing in-depth analysis with real-time detection

Payment service providers aim to avoid delays in legitimate transactions, which can affect customer satisfaction and lead to churn. Therefore, there is a critical need to gather, process, and analyze vast amounts of data more quickly than ever before.



Technological advances increase risk of fraud

With more sophisticated purchasing methods, the threat of fraud has significantly grown. The challenges posed by AI-enabled fraud is a top concern for payment service providers, financial institutions, and even governments.⁴ Vigilance, collaboration, and strategic responses are essential to combat this escalating menace.

A robust fraud detection approach must adapt to these challenges by focusing on three key components. This approach not only improves security and compliance but also enhances operational efficiency and customer trust.

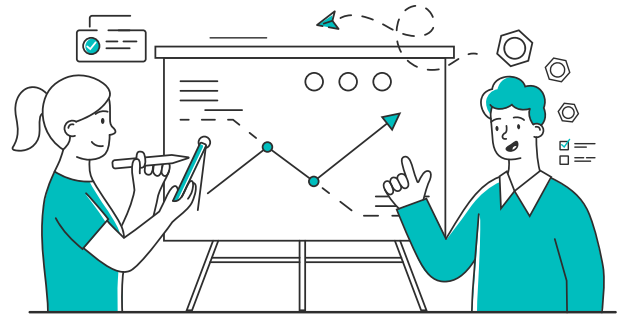
New directives

Incorporating innovations such as open banking, ISO 20022, and advancements in cross-border payments is essential to staying ahead of regulatory and market demands. Open banking allows for more integrated and customer-centric services by enabling third-party providers to access banking information. ISO 20022 provides a common language for global financial communications, facilitating better data quality and interoperability. Cross-border payment advancements ensure that transactions are efficient, transparent, and secure on an international scale. By adopting these new directives, payment service providers can create a more secure and seamless payment experience for their customers.

Strategy

Implementing strong data governance, transformation processes, lineage, and cataloging is crucial for ensuring data integrity and traceability. Data governance establishes robust security measures, access controls, and encryption techniques to safeguard sensitive customer information, ensuring compliance with regulations such as General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS). Transformation processes ensure that data is accurately converted and managed throughout its lifecycle. Defining data lineage helps in mapping data transformations from

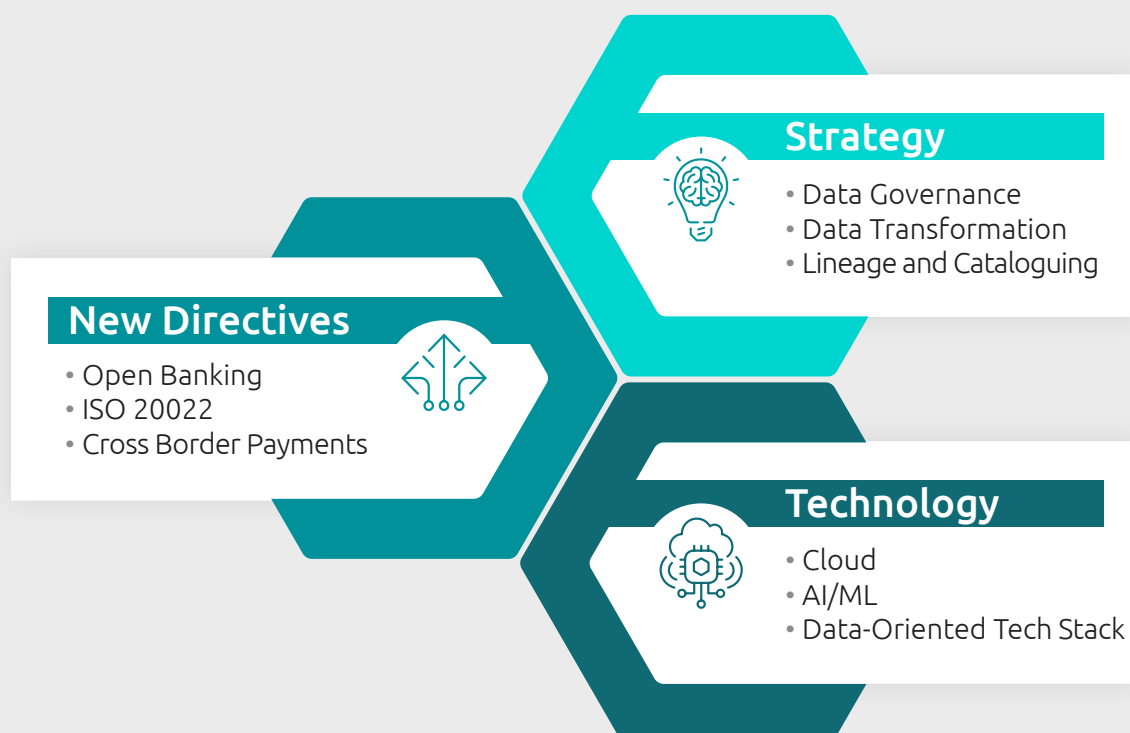
source to destination, which is vital for auditing and compliance. A dynamic data catalog captures payment data entity definitions, providing a trusted foundation for data discovery and operational rigor.



Technology

Leveraging cutting-edge technologies such as cloud computing, AI, ML, and a data-oriented tech stack significantly enhances fraud detection capabilities and response times. Cloud computing offers scalability, flexibility, and robust infrastructure to handle large amounts of payment data. AI and ML algorithms can analyze patterns and detect anomalies in real-time, reducing false positives and improving accuracy. A data-oriented tech stack ensures that all technological components are aligned to support efficient data processing and analysis, facilitating faster and more effective fraud detection.

Figure 2: The three critical components of a robust fraud detection approach



Three-step approach to prevent fraud and future-proof your organization

Using the three key components as a foundation, Capgemini and MongoDB have developed a comprehensive three-step approach to prevent fraud. This approach is designed to integrate seamlessly within various payment messaging

infrastructures, including the Clearing House Automated Payment System (CHAPS), Single Euro Payments Area (SEPA), Faster Payments, and other cross-border payment transactions.

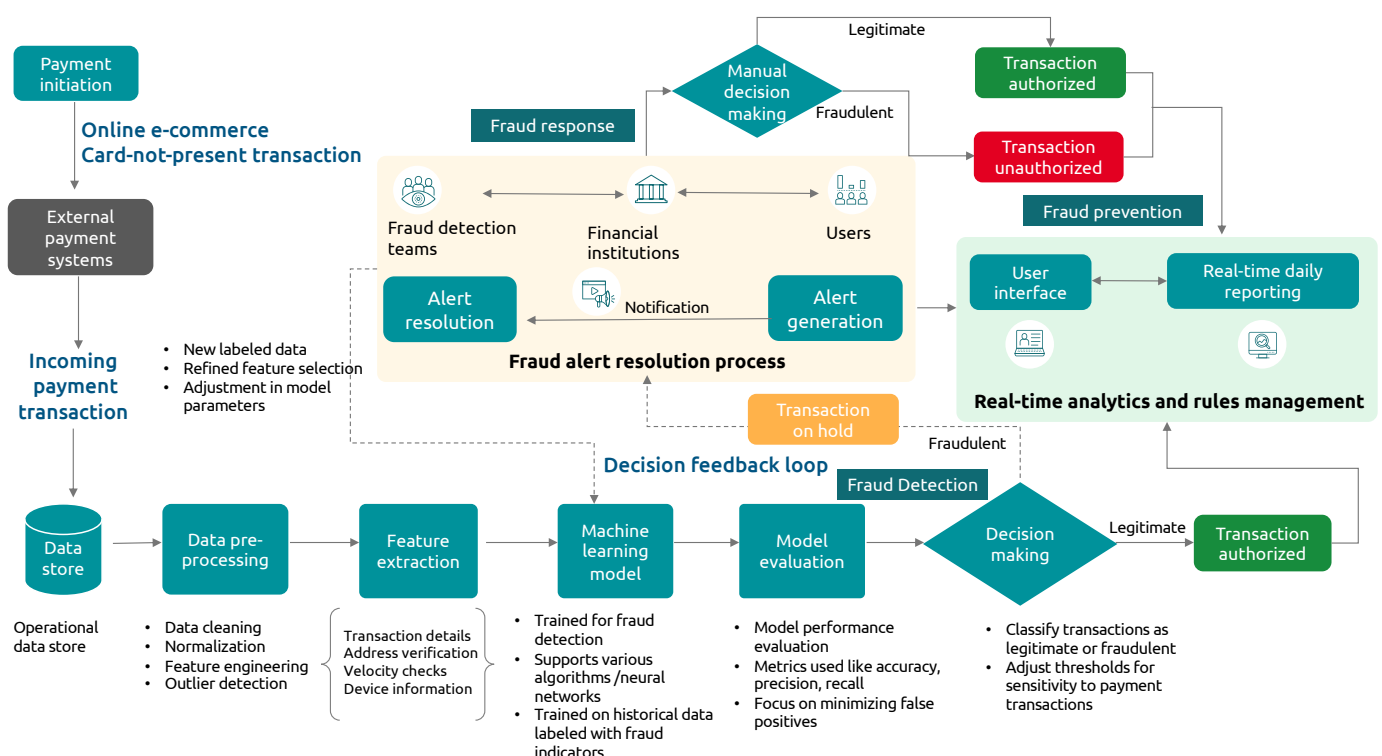
Figure 3: Three-step approach to preventing fraud



Our approach future-proofs organizations by continuously evolving through a dynamic ML model. This model harnesses the extensive range of data

attributes available through the ISO 20022 message format, enhancing its ability to detect and prevent fraudulent activities more effectively.

Figure 4: Overview of the three-step approach in action



Step 1

Real-time fraud detection in card-not-present transactions

When onboarding to ISO 20022, organizations can leverage the structured data attributes to build robust detection models capable of preventing fraudulent activities. The table below lists these attributes, the types of validation approaches that can be used to detect fraud, and the typical pattern analysis associated with these validations. While these attributes are indicative, organizations can select the most relevant ones based on their specific needs for the ML model.

Figure 5: Data attributes on a payment transaction that are critical for fraud detection

Data entity type	Data entity subtype	Validation approach	Pattern analysis
Transaction details	Transaction amount	Threshold check	Amount exceeds typical threshold set
	Currency	Cross referencing	<ul style="list-style-type: none"> Unusual currency conversion Mismatched geography pattern Currency fluctuations arbitrage
	Transaction date/time	Cross referencing	<ul style="list-style-type: none"> Temporal patterns to see for spikes or dips Velocity checks Transaction sequencing
	Transaction type	Cross referencing	Behavioral analysis
Participant identification	Sender header identifiers	Cross referencing	<ul style="list-style-type: none"> Deviation to KYC compliance Issues in transaction reconciliation
	Receiver header identifiers	Cross referencing	<ul style="list-style-type: none"> Deviation to KYC compliance Issues in transaction reconciliation
Payment references	Invoice number	Reconciliation check	Anomaly detection
	Payment reference number	Reconciliation check	Anomaly detection
	Customer ID	Reconciliation check	Anomaly detection
Message authentication	Message authentication code (MAC)	Check to prevent tampering	Error alerts during difference in computed MAC versus received MAC
	Cryptographic digital signatures	Check to prevent tampering	Error alerts during difference in computed MAC versus received MAC
Payment routing information	Intermediary banks	Check for deviation from pattern	Inconsistent routing or deviation to PCI DSS compliance
	Payment processors	Check for deviation from pattern	Inconsistent routing or deviation to PCI DSS compliance
Payment status and confirmation	Status updates	Real-time monitoring	Sudden change in status like delay in settlement or rejection
	Confirmation codes	Real-time monitoring	Sudden change in status like delay in settlement or rejection



Each incoming transaction is assigned a risk weight based on a combination of data attributes. These risk weights are then evaluated against a set of predefined rules to determine whether the transaction should be approved or declined. For example, here are some rules that can be implemented:



Transaction details

Transactions exceeding a predefined threshold, such as those above a cardholder's typical range of \$5,000-\$10,000, are flagged as potentially fraudulent. These thresholds are set based on local regulations and organizational control systems. However, monitoring transaction amounts alone is insufficient. The complexities of data analysis and the limitations of controls pose challenges in effectively managing and detecting structuring.



Address verification

Utilizing an address verification service for cards based in the US, UK, and Canada. Incoming transactions are rejected if an invalid address is detected.



High-risk countries

Transactions originating from or involving countries known for high levels of money laundering activities are flagged for additional scrutiny. Enhanced monitoring can aid in better tracking the involvement of high-risk countries at both the transaction's origin and its endpoint.



Velocity checks

Monitoring for frequent transactions with similar attributes. Examples include:

- If the number of transactions at a specific billing address exceeds five.
- If the number of email addresses associated with a given card exceeds a specific threshold within a billing cycle.
- Frequent transactions with similar attributes within a short period.



Deviation

Identifying discrepancies between expected values and the actual values present in participant information.

The ML algorithm assigns a risk score to each transaction on a scale of 0 to 100, where 0 indicates the least risk and 100 indicates the highest risk. This score is determined based on the values of the relevant data attributes present in the incoming transaction.

Step 2

Real-time fraud prevention powered by MongoDB

The technology that goes behind a highly adaptable and accurate fraud detection and prevention engine is crucial. Figure 6 represents a real-time, event-driven architecture designed to combat fraud. When this architecture pattern is applied to CNP transactions, the data flow and process are as follows:

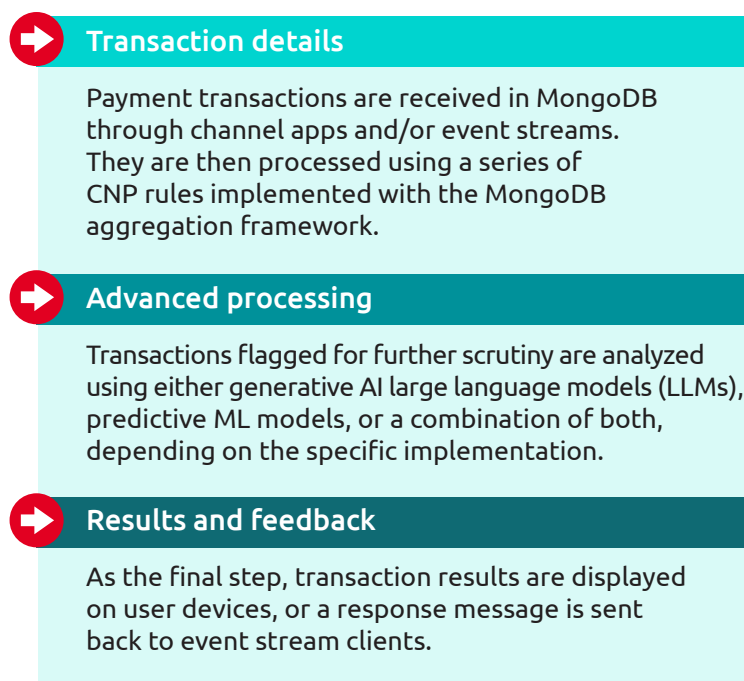
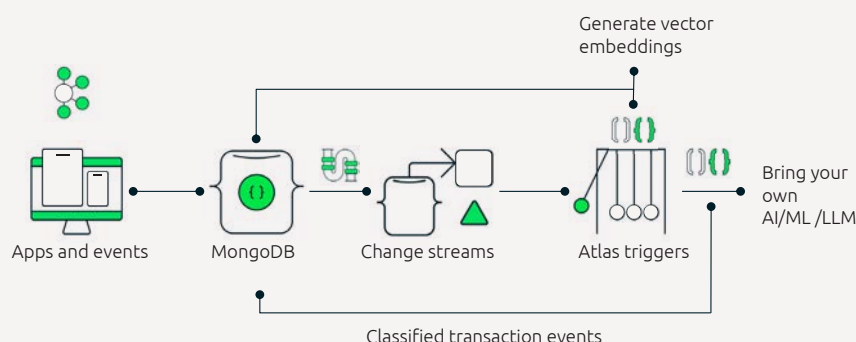


Figure 6: Real-time event-driven fraud detection and prevention system architecture using MongoDB.



MongoDB platform features that make it a strong choice for a fraud detection framework

The flexibility of MongoDB's document model is perfectly suited to the diverse nature of payment schemes. It allows for the seamless addition of new payment methods at the request of customers, with no downtime and a faster response time.

Compliance support for regulations such as GDPR, PCI, California Consumer Privacy Act (CCPA), and Payment Services Directive 2 (PSD2) which are crucial in the finance sector. MongoDB's native **security features** ensure that data handling meets these regulatory standards, protecting sensitive customer information and transaction data. Enhanced authentication and role-based authorization controls further fortify the system against unauthorized access, a common entry point for fraudsters.

Change streams enable real-time monitoring of database changes. In fraud prevention, this means immediate detection of suspicious activities or transactions. By receiving instant notifications, fraud prevention teams can quickly respond to potential threats, reducing the window of opportunity for fraudsters.

The **aggregation framework** allows for complex data processing and analytics directly within the database. This capability is crucial for implementing sophisticated, rules-based fraud detection algorithms. By processing transactions in real time, MongoDB can identify and flag anomalies or suspicious patterns indicative of fraud.

AI and ML are at the forefront of modern fraud detection. MongoDB's integration capabilities enable organizations to implement advanced **AI models** for detecting complex fraud patterns. This flexibility enables continuous learning and adaptation to new and evolving fraud techniques.

In an increasingly mobile world, the ability to sync data and notifications in real time across devices is crucial. **Atlas Device Sync** ensures that fraud alerts and notifications are delivered instantly to mobile devices, enabling a swift response, whether it's freezing a compromised card or contacting a customer for verification.

Step 3

Real-time fraud response strategy

Visualization tools, such as charts and reporting capabilities, are essential for monitoring and analyzing transaction data. They enable support center personnel to quickly understand and react to data trends, unusual activities, and potential threats. Efficient reporting tools aid in decision-making and help maintain a high level of vigilance against fraud.

User behavior analytics (UBA) is critical for understanding user behavior, login patterns, device usage, and transaction timing to identify anomalies. Collecting and analyzing user behavior data raises privacy concerns that must be addressed to ensure compliance with data protection regulations like GDPR, CCPA, and PCI, especially for payments processing.

In addition to rule-based fraud detection, UBA helps reduce false positives by focusing on individual user behavior, thereby increasing the accuracy of detecting fraudulent transactions. Combining UBA with behavioral biometrics, such as keystroke dynamics and mouse movements, further enhances accuracy.



Case Study

Modernizing credit card fraud monitoring for a prominent UK bank

A leading UK bank embarked on a comprehensive payments modernization program to stay future-ready, which included compliance with ISO 20022 standards, migrating payment flows to a strategic architecture, and decommissioning legacy systems. These changes were vital to enhance the bank's operational resilience, address the growing risk of fraud, and meet new regulatory requirements.



Our solution

The bank implemented a comprehensive strategy to modernize their payment infrastructure, focusing on several key areas:

- **Strategic multi-stage migration:** A multi-stage strategy to migrate legacy payment channels to the new strategic architecture was implemented, ensuring minimal disruption and steady progress towards full compliance.
- **Enhanced data utilization:** By analyzing industry requirements and developing solutions to handle enhanced data, the bank took full advantage of ISO 20022's benefits, such as improved straight through processing (STP) rates and richer payment data.
- **Compliance and future-readiness:** The strategy included ensuring compliance with current regulations and the flexibility to adapt to new requirements quickly and cost-effectively.



Impact delivered

- By migrating legacy payment channels to a new strategic architecture, the bank ensured that the latest security protocols and fraud detection mechanisms were in place, significantly reducing vulnerabilities that could be exploited in older systems.
- With enhanced data handling capabilities, the bank can now analyze transaction data more effectively, identifying unusual patterns and potential fraud with greater accuracy. This capability supports advanced analytics and machine learning models for real-time fraud detection.
- Ensuring compliance with current regulations such as GDPR, CCPA, and PCI keeps the bank aligned with the latest security standards. This proactive approach helps maintain robust defenses against fraud while remaining adaptable to future regulatory changes and emerging fraud techniques.



Upgrade your fraud detection capabilities with Capgemini and MongoDB

Capgemini and MongoDB can help transform your payments processing platform with a modern data infrastructure powered by a robust fraud detection framework. By leveraging our expertise and MongoDB's cutting-edge technology, we can help you achieve significant benefits, especially in CNP transactions including:



Protection of financial assets

As payment service providers continue to grow, the threat from fraud and the subsequent erosion of financial assets increase proportionally. Early detection and prevention can help avoid these setbacks.



Reducing bogus chargebacks

Improved fraud detection can mitigate fraudulent chargebacks. These chargebacks not only result in revenue and merchandise losses for merchants but also consume significant time and energy to resolve disputes.




Elevating reputation standards and customer loyalty

A robust fraud detection and prevention framework enhances customer trust. This is especially important for marketplace-style businesses where reputation is paramount.



Compliance with regulations

Adhering to regulations helps avoid penalties, fines, and breaches, saving organizations from unnecessary waste of time, effort, and money.



Don't let fraud compromise your operations. Contact us to learn how we can help your organization build a secure, efficient, and modern fraud detection approach.

Contacts

Please reach out to us with questions or to schedule a conversation about this paper's content and our capabilities to assist your organization.

Capgemini



Arindam Choudhury

EVP, Banking & Capital Markets Head
Financial Services Insights & Data
arindam.choudhury@capgemini.com



Saurabh Deshmukh

Sr. Director, UK Head of Banking
and Capital Markets
Financial Services Insights & Data
saurabh.deshmukh@capgemini.com



Saurabh Khandelwal

Senior Manager
Financial Services Insights & Data
saurabh.c.khandelwal@capgemini.com

MongoDB



Shiv Pullepu

Industry Principal, Financial Services
MongoDB Inc
shiva.pullepu@mongodb.com



Data-powered financial services

Learn how we can help your organization harness the power of data using AI, machine learning, process automation, and more.



About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com

About MongoDB

MongoDB's modern, multi-cloud database offers significant architectural advantages by enabling organizations to securely unify application data (both structured and unstructured) with AI-related data (vectors). This capability allows institutions to build rich, real-time AI applications. At the core is MongoDB Atlas, the most advanced multi-cloud database on the market. Atlas provides unmatched data distribution and cloud mobility, built-in automation for resource and workload optimization, and a flexible document model, among other features. MongoDB also offers the flexibility to deploy applications on-premises, on a single public cloud, or across multiple clouds simultaneously, ensuring resilience, scalability, and the highest levels of data privacy and security.

For more information, please visit www.mongodb.com

© Copyright 2024 Capgemini. All rights reserved.

