Global Fraud Detection and Prevention in BFSI Market Assessment, By Offerings [Solutions, Services], By Fraud Type [Identity Theft, Payment Fraud, Money Laundering, Insurance Fraud, Others], By Deployment Mode [On-premises, Cloud-based], By End-use [Banks, Insurance Company, NBFCs, Credit Unions, Others], By Region, Opportunities and Forecast, 2018-2032F

Market Report | 2025-07-31 | 232 pages | Market Xcel - Markets and Data

AVAILABLE LICENSES:

- Single User License $4800.00
- Muti-User/Corporate Licence $6000.00
- Custom Research License $8500.00

Report description:

Global fraud detection and prevention in BFSI market is projected to witness a CAGR of 20.11% during the forecast period 2025-2032, growing from USD 37.58 billion in 2024 to USD 162.71 billion in 2032. The fraud detection and prevention (FDP) in BFSI (Banking, Financial Services, and Insurance) market is experiencing a strong growth trajectory due to the rapid digitization of financial services, the increasing number of cyber fraud incidents, and the growing need to secure sensitive customer data.
The global fraud detection and prevention (FDP) in Banking, Financial Services, and Insurance (BFSI) market is on the path to continued rapid growth, primarily driven by the increased complexity and frequency of digital fraud across digital channels. With the acceleration towards digital banking, online insurance claims, real-time payment systems, organizations are facing increased exposure to cyber fraud, identity theft, payment fraud, account takeovers, and data leaks.
To adapt to the rapidly evolving, technologically advanced landscape of fraud, financial institutions are moving toward FDP solutions using a combination of artificial intelligence (AI), machine learning (ML), big data analytics, and behavioral biometrics that allow for real-time fraud detection, risk-based authentication, and predictive analytics to reduce financial crimes. Additionally, global regulatory structures require financial institutions to comply with and invest in fraud prevention infrastructure to meet compliance frameworks, such as Know Your Customer (KYC), Anti-Money Laundering (AML), and the General Data Protection Regulation (GDPR), which has led to increased growth in the FDP market.
Moreover, the increased adoption of cloud-based fraud detection platforms that can scale, offer cost-effective solutions, and provide easier APIs has created a growing demand for fraud detection, particularly against cloud-based accounts. As organizations

strive to protect customer trust and comply with KYC legislation (especially during the pandemic), the rising demand for next-generation fraud detection systems is expected to persist.

For instance, on 11 March 2025, Arab National Bank (ANB) partnered with IBM Corporation and EJADA to implement IBM Safer Payments, adopting cross-channel fraud protection capabilities to protect and empower its customers with easier access to the latest secure and innovative banking experiences.

Rapid Digitalization of Financial Services Drives Market Demand

The rapid digital transformation of the banking, financial services, and insurance (BFSI) sector has emerged as a significant contributor to the global fraud detection and prevention (FDP) market. With an increasing number of customers wanting easy access and remote services offered by financial institutions, customers are adopting digital banking functions, mobile payments, online lending and digital insurance to meet those expectations, increasing the amount and pace of financial transactions online. As organizations digitize to improve service and make operations more efficient, this transformation also creates more risk. Financial systems are vulnerable to cyber issues as reliance on digital, internet-based platforms continues to increase. Cyber fraud has increased, with instances of identity theft, phishing, malware, and account takeover. More sophisticated cybercriminals have adopted advanced attacks against vulnerabilities in digital channels. Increasing risk, impact, and sophistication of attacks are becoming more significant for organizations and their customers. As a response, financial organizations are becoming increasingly investment-conscious about using advanced fraud detection and prevention solutions that monitor in real-time, offer behavioral analysis, predictive threat detection, and are even expanding to include authentication and account lifecycle management. Several financial organizations have begun to seek new technology solutions to enhance their fraud management systems by incorporating artificial intelligence (AI), machine learning (ML), and data analytics, aiming to improve accuracy, speed, and the ability to identify and respond to various types of threats.

For example, in December 2024, the Reserve Bank of India (RBI) launched MuleHunter.ai, an AI-powered tool that verifies mule accounts used in digital banking frauds. As digital transactions increased on platforms such as UPI and mobile banking, cyber frauds also skyrocketed. The system employs AI/ML that analyzes real-time transaction patterns and identifies suspicious ones, in part because the rapid financial digitalization means more intelligent fraud prevention strategies are needed.

Rising Incidence of Sophisticated Cyber Threats Drives Market Growth

The rapid frequency and sophistication of cyber threats have become an important growth driver for the global Fraud Detection and Prevention (FDP) market across the BFSI sector. Financial institutions are facing an increasing number of frauds perpetrated by more sophisticated methods like phishing, identity theft, account takeovers, synthetic identity fraud, and ransomware, as well as increasingly sophisticated threats that involve advanced techniques such as deepfake identities, organized crime, social engineering, AI generated scams and coordinated bot actions, thus moving beyond traditional methods. These cybercrimes can bypass traditional security controls, causing financial losses, operational downtime, and ultimately harming the organization by eroding trust with its customers. The increase in digital offerings, as well as third-party integrations, has expanded the attack surface, thereby increasing the likelihood of unauthorized access and fraudulent transactions. To combat advanced fraud schemes, BFSI organizations are increasingly utilizing intelligent FDP, which incorporates artificial intelligence (AI), machine learning (ML), and big data analytics to offer real-time anomaly detection, risk scoring, and adaptive authentication, enabling proactive handling of emerging threats. In addition, legislation worldwide is tightening compliance requirements for control frameworks related to protecting consumer data and prohibiting fraudulent activities. As increased activity continues to change the threat landscape, financial institutions are investing heavily in reducing cyber threats through advanced FDP solutions.

For example, in November 2024, IBM Corporation Security expanded its Trusteer Pinpoint Detect solution to give customers advanced behavioral biometrics capabilities to detect account takeover attempts in real-time. The platform monitors a user's interactions, such as mouse movements and clicks, to build unique behavioral models and detect anomalies, even when they are using valid credentials. This advancement has made it easier for companies to detect more advanced types of threats, such as credential theft and social engineering attempts, demonstrating a trend where fraud prevention tools are increasingly utilizing AI in the banking, financial services, and insurance (BFSI) market.

Cloud Deployment Segment Dominates Market Growth

The cloud deployment segment is projected to be a high-growth segment of the global Fraud Detection and Prevention (FDP) market, with a steady growth trend observed in the broader BFSI segment of FDP. With financial institutions actively pursuing

their digital transformation programs, there is a significant shift toward cloud deployment, offering the benefits of scalability, cost efficiency, and the ability to support real-time fraud detection and monitoring. Cloud FDP systems enable banks, insurance companies, and fintechs to implement more sophisticated analytics, AI, and ML capabilities without incurring significant infrastructure investments. They also allow faster response to fraud trends, automatic upgrades, and integration with third-party systems and mobile banking feeds. As banks, payments, and insurance companies continue to adopt a more digital business model, the rise in remote transactions, mobile payments, and online banking offerings has fueled the demand for more flexible and agile fraud prevention methods. Cloud deployment also encourages centralized threat intelligence, encourages inter-location or inter-department collaboration, and can provide a well-rounded posture to improve the overall security stance of banks, insurance companies, and fintechs that operate under. While financial institutions continue to pursue real-time processing of data in compliance with regulatory requirements, with risk management aiding in effective strategy and business models, cloud deployment is poised for rapid adoption across the BFSI sector.

For instance, in August 2024, Rippleshot, Inc. announced a partnership with CPI Card Group to integrate its cloud-based, AI-enabled fraud detection platform into CPI's payment card services. The collaboration aims to enhance security, reduce the cost of fraud, and naturally increase customer retention, while highlighting the growing adoption of scalable, cloud-native fraud detection platforms (FDPs) within the payments and card ecosystem.

North America Dominates the Global Fraud Detection and Prevention in BFSI Market Size

North America occupies the top position in terms of share in the world's fraud detection and prevention (FDP) market share in the Banking, Financial Services and Insurance (BFSI) sector driven by key factors such as high uses of digital banking, consolidated financial infrastructure and the first adopters of new and innovative methods including artificial intelligence (AI), machine learning (ML) and cloud-based fraud detection system. The region also suffers from a high rate of difficult-to-detect cyber threats, including the everyday online and mobile banking activity, phishing, account takeover, identity theft and synthetic fraud, and, as a result, financial institutions in the U.S. and Canada have invested heavily into real-time fraud detection tools and multiple security mechanisms to protect customer data and the integrity of an effective transactions.

In addition to high use of digital banking accounts and the high internet use through all channels of the customer experience, different and applicable regulations such as the Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry Data Security Standard (PCI DSS), laws around data protection and regulations through the Federal Reserve and other institutions such as FINRA, have not only prompted BFSI type organizations to strengthen their fraud systems - they have advanced and accelerated their use of sophisticated fraud prevention technology.

For instance, in April 2025, JPMorgan Chase & Co. launched NeuroShield, an AI-driven fraud detection service using behavioral biometrics and real-time analytics to combat digital banking fraud. It was reported that NeuroShield reduced fraud losses by 40% through the pilot project. The announcement highlights North America's significant lead in the adoption of advanced fraud detection and prevention (FDP) solutions, driven by high volumes of digital transactions, stringent regulatory requirements, and substantial capital investments.

Key Players Landscape and Outlook

The Fraud Detection and Prevention (FDP) industry, particularly in the banking, financial services, and insurance (BFSI) sector, strikes a good balance between innovation and competition. This has prompted companies to innovate and invest a significant amount of money in new and emerging technologies to combat complex fraud threats proactively. Companies in this space include major players such as IBM, FICO, SAS, BAE Systems, NICE Actimize, Oracle, SAP, and ACI Worldwide, which have developed AI- and machine learning‐based fraud management solutions specifically designed to address the needs of banking and insurance organizations. Solutions are being developed that focus on real-time risk scoring, behavioral biometrics, cloud-native capabilities, and end-to-end fraud analytics. The outlook remains positive; demand for intelligent, scalable, and regulatory-compliant FDP systems continues to grow, especially in the larger regions of North America, Europe and Asia-Pacific. Over the next five years, the competitive landscape will be influenced by several factors, including new strategic alliances, cloud adoption, and AI-enabled solutions, as well as the increasing demand for FDP from fintechs, neobanks, and mid-tier BFSI organisations.

For instance, in June 2025, NICE Ltd. announced that KeyBank, a central US bank-based financial institution, is further enhancing its financial crime operations by implementing its X-Sight AI Enterprise Platform. The X-Sight AI Enterprise Platform is a

cutting-edge solution that leverages analytics and AI to address critical issues in fraud detection, compliance, and risk management. The implementation complemented KeyBank's modernization efforts in crime prevention infrastructure. The move reflects a broader trend among large financial institutions to invest in intelligent, scalable fraud prevention technologies.

Table of Contents:

1.Project Scope and Definitions
2.Research Methodology
3.Executive Summary
4.Voice of Customers
4.1.Respondent Demographics
4.2.Awareness of Fraud Detection and Prevention Software in BFSI
4.3.Adoption Challenges Faced by BFSI Institutions
4.4.Key Drivers and Adoption
5.Global Fraud Detection and Prevention in BFSI Market Outlook, 2018-2032F
5.1.Market Size Analysis & Forecast
5.1.1.By Value
5.2.Market Share Analysis & Forecast
5.2.1.By Offerings
5.2.1.1.Solutions
5.2.1.2.Services
5.2.2.By Fraud Type
5.2.2.1.Identity Theft
5.2.2.2.Payment Fraud
5.2.2.3.Money Laundering
5.2.2.4.Insurance Fraud
5.2.2.5.Others
5.2.3.By Deployment Mode
5.2.3.1.On-premises
5.2.3.2.Cloud-based
5.2.4.By End-use
5.2.4.1.Banks
5.2.4.2.Insurance Company
5.2.4.3.NBFCs
5.2.4.4.Credit Unions
5.2.4.5.Others
5.2.5.By Region
5.2.5.1.North America
5.2.5.2.Europe
5.2.5.3.Asia-Pacific
5.2.5.4.South America
5.2.5.5.Middle East and Africa
5.2.6.By Company Market Share Analysis (Top 5 Companies and Others - By Value, 2024)
5.3.Market Map Analysis, 2024
5.3.1.By Offerings
5.3.2.By Fraud Type
5.3.3.By Deployment Mode
5.3.4.By End-use

5.3.5.By Region
6.North America Fraud Detection and Prevention in BFSI Market Outlook, 2018-2032F
6.1.Market Size Analysis & Forecast
6.1.1.By Value
6.2.Market Share Analysis & Forecast
6.2.1.By Offerings
6.2.1.1.Solutions
6.2.1.2.Services
6.2.2.By Fraud Type
6.2.2.1.Identity Theft
6.2.2.2.Payment Fraud
6.2.2.3.Money Laundering
6.2.2.4.Insurance Fraud
6.2.2.5.Others
6.2.3.By Deployment Mode
6.2.3.1.On-premises
6.2.3.2.Cloud-based
6.2.4.By End-use
6.2.4.1.Banks
6.2.4.2.Insurance Company
6.2.4.3.NBFCs
6.2.4.4.Credit Unions
6.2.4.5.Others
6.2.5.By Country Share
6.2.5.1.United States
6.2.5.2.Canada
6.2.5.3.Mexico
6.3.Country Market Assessment
6.3.1.United States Fraud Detection and Prevention in BFSI Market Outlook, 2018-2032F*
6.3.1.1.Market Size Analysis & Forecast
6.3.1.1.1.By Value
6.3.1.2.Market Share Analysis & Forecast
6.3.1.2.1.By Offerings
6.3.1.2.1.1.Solutions
6.3.1.2.1.2.Services
6.3.1.2.2.By Fraud Type
6.3.1.2.2.1.Identity Theft
6.3.1.2.2.2.Payment Fraud
6.3.1.2.2.3.Money Laundering
6.3.1.2.2.4.Insurance Fraud
6.3.1.2.2.5.Others
6.3.1.2.3.By Deployment Mode
6.3.1.2.3.1.On-premises
6.3.1.2.3.2.Cloud-based
6.3.1.2.4.By End-use
6.3.1.2.4.1.Banks
6.3.1.2.4.2.Insurance Company

6.3.1.2.4.3.NBFCs
6.3.1.2.4.4.Credit Unions
6.3.1.2.4.5.Others
6.3.2.Canada
6.3.3.Mexico
*All segments will be provided for all regions and countries covered
7.Europe Fraud Detection and Prevention in BFSI Market Outlook, 2018-2032F
7.1.Germany
7.2.France
7.3.Italy
7.4.United Kingdom
7.5.Russia
7.6.Netherlands
7.7.Spain
7.8.Turkey
7.9.Poland
8.Asia-Pacific Fraud Detection and Prevention in BFSI Market Outlook, 2018-2032F
8.1.India
8.2.China
8.3.Japan
8.4.Australia
8.5.Vietnam
8.6.South Korea
8.7.Indonesia
8.8.Philippines
9.South America Fraud Detection and Prevention in BFSI Market Outlook, 2018-2032F
9.1.Brazil
9.2.Argentina
10.Middle East and Africa Fraud Detection and Prevention in BFSI Market Outlook, 2018-2032F
10.1.Saudi Arabia
10.2.UAE
10.3.South Africa
11.Demand Supply Analysis
12.Value Chain Analysis
13.Porter's Five Forces Analysis
14.PESTLE Analysis
15.Market Dynamics
15.1.Market Drivers
15.2.Market Challenges
16.Market Trends and Developments
17.Regulatory Fines Avoided through Solution Adoption (Best Effort Basis)
18.Case Studies
19.Competitive Landscape
19.1.Competition Matrix of Top 5 Market Leaders
19.2.SWOT Analysis for Top 5 Players
19.3.Key Players Landscape for Top 10 Market Players
19.3.1.FICO

19.3.1.1. Company Details
19.3.1.2. Key Management Personnel
19.3.1.3. Products and Services
19.3.1.4. Financials (As Reported)
19.3.1.5. Key Market Focus and Geographical Presence
19.3.1.6. Recent Developments/Collaborations/Partnerships/Mergers and Acquisition
19.3.2. NICE Ltd. (NICE Actimize)
19.3.3. SAS Institute Inc.
19.3.4. ACI Worldwide
19.3.5. BAE Systems
19.3.6. Experian plc
19.3.7. IBM Corporation
19.3.8. LexisNexis Risk Solutions
19.3.9. RSA Security LLC
19.3.10. FIS (Fidelity National Information Services, Inc.)
*Companies mentioned above DO NOT hold any order as per market share and can be changed as per information available during research work.
20. Strategic Recommendations
21. About Us and Disclaimer

Global Fraud Detection and Prevention in BFSI Market Assessment, By Offerings [Solutions, Services], By Fraud Type [Identity Theft, Payment Fraud, Money Laundering, Insurance Fraud, Others], By Deployment Mode [On-premises, Cloud-based], By End-use [Banks, Insurance Company, NBFCs, Credit Unions, Others], By Region, Opportunities and Forecast, 2018-2032F

Market Report | 2025-07-31 | 232 pages | Market Xcel - Markets and Data

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4800.00
	Muti-User/Corporate Licence	$6000.00
	Custom Research License	$8500.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	

Address*		City*	
Zip Code*		Country*	
		Date	2026-03-02
		Signature	