

# FINsights

Technology Insights for the Financial Services Industry

ENTERPRISE  
PAYMENTS



## IN THIS ISSUE

- Mobile Banking and Payments Security and Usability: What's in Your Mobile Wallet?
- Innovation in Retail Payments • Electronic Invoicing: How to Increase E-Invoicing B2B Transactions

Infosys®

POWERED BY INTELLECT  
DRIVEN BY VALUES

# CONTENTS

Preface

From the Editor's Desk

## Retail Payments

- |  |    |
|--|----|
| 1. Innovation in Retail Payments   | 5  |
| 2. Mobile Payments: Sustainability of Business Models                                  | 15 |
| 3. Payment Cards: Trends, Challenges and Innovations                                   | 25 |
| 4. Mobile Banking and Payment Security and Usability:<br>What's in Your Mobile Wallet? | 35 |

## Wholesale Payments

- |   |    |
|---|----|
| 5. Wholesale Payments: Trends and Transformation  | 43 |
| 6. Electronic Invoicing: How to Increase E-Invoicing B2B<br>Transactions                                  | 49 |
| 7. Centralizing Wholesale Payment Services: The Key to<br>Improved Growth, Efficiency and Risk Management | 55 |
| 8. Money Movement Automation: A Case Study  | 69 |
| 9. Financial Institution Opportunities in Healthcare Revenue<br>Cycle Management                          | 73 |

## Payments Transformation

- |   |     |
|---|-----|
| 10. Enterprise Payments: Breaking Barriers          | 83  |
| 11. Top Transformational Trends in Check Processing | 95  |
| 12. SEPA: Outsourcing - The Key to Changing Times   | 109 |
| 13. Payments Fraud                                  | 121 |



# 13

## PAYMENTS FRAUD

- DEBASHIS PRADHAN
- NAVEEN BALAWAT

The financial services industry has undergone tremendous change facilitated by the ease with which firms can transfer money using different payment methods and channels. However, this change has also resulted in rise of fraud and the potential ways in which this could be perpetrated in the industry.

Though firms have been relatively successful in fending off some of the obvious forms of attack, they continue to lose billions of dollars to fraud. This fight has been hampered by disjointed efforts to tackle fraud and an increasing sophistication in which fraudsters now operate.

We believe firms should take a holistic view to tackle fraud comprehensively. The first step to this approach is to establish a centralized fraud management unit to set the direction, and bring together disjointed anti-fraud efforts across the enterprise. Governance mechanism helps to standardize policies and controls across the firm. Secondly, firms should adopt a risk-based approach to identify payment areas that need most attention. Finally, they need to invest in bringing together fraud monitoring systems, improving them at better at detecting and catching fraud as it happens and identifying cross - channel fraud.

## To Catch a Thief

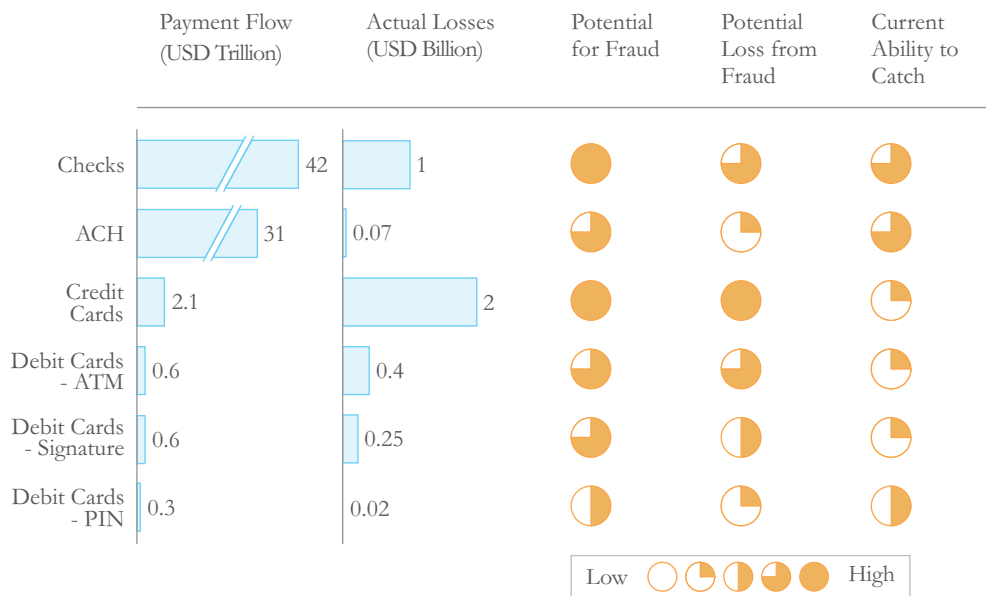
The payments landscape in the US banking industry has radically changed with the advent of the electronic age. The means of paying money has continued to evolve from traditional paper-based instruments like cash and checks, to more electronic options like Automated Clearing House (ACH) or cards. This has been largely driven by a change in customer preferences, evolution of technology and the entry of non-banking players. In an era of competition and declining margins, banks have begun to introduce products and services faster than

ever. They have also been quick in adopting newer channels of payments. This has opened them up to a greater risk of payment fraud than ever before. Independent surveys show that payments fraud is pervasive and increasing.

Fraudsters are an ingenious lot. They have become more sophisticated and organized in their use of technology and are also well funded. Their tools of trade have also improved with the introduction of new products and services. Ways to commit fraud are gaining diversity and are no longer limited to a single channel or mode of payment.

### Key Payment Methods and Losses

Fig - 1



Fraud statistics vary from source to source due to differences in approach and definition of fraud. The numbers in this chart are only meant to provide a relative comparison of the size of fraud across payment methods.

#### Sources:

2007 Federal Reserve Payments Study  
 2007 ABA Deposit Fraud Survey  
 Financial Insights, Celent, Gartner  
 Visa, MasterCard  
 PULSE 2007 Debit Issuer Study  
 Infosys Analysis

Moreover, with the growth in electronic channels and alternate modes of payment, fraudsters are getting better at evasion by layering their transactions through multiple channels. Needless to say, financial services firms have a tough task keeping pace with the Al Capones and staying a step ahead of them.

### **Identifying Chinks in the Armor**

Key to devising a strategy to tackle fraud is to first understand the various payment methods and evaluate how prone they are to attack. Large financial services firms with multiple business lines and payments channels are more at risk to attack than smaller firms, though the smaller firms are more likely to incur losses. Since not all payment methods are targeted equally, it's important for firms to evaluate payment mechanisms at work and identify the most prominent chinks in their armor.

### **Check Fraud**

Checks remain one of the most targeted areas for fraud. Check fraud could be perpetrated in many different ways - payee name could be altered, checks could be counterfeited, or paychecks could be lost or stolen.

Though the volume of checks written has declined over the years, check fraud has actually increased with a corresponding increment in actual losses. However, firms have been able to avoid large financial losses as their systems and controls have been able to catch most of the fraudulent activity.

### **ACH Fraud**

ACH payments have long been virtually free of fraudulent activity. But, they are fast losing this immunity as new ways to authorize debits are being misused. New ACH class codes now permit people to authorize ACH debits over the phone or the web and allow checks to be

converted into ACH debits at either the Point-of-Sale (POS) or retail lockbox. Some of the more sophisticated scams arise from telemarketers who tape-record customer ACH authorizations on the phone, and either use it to initiate ACH debits or sell the information to other companies. Not surprisingly, consumer accounts bear the brunt of such cross-channel attacks.

On the other hand, businesses have a short unauthorized ACH return window and a greater potential for loss due to higher balances being retained in accounts.

While the actual losses from ACH fraud is relatively low, companies spend a significant amount of time and money returning fraudulent ACH debits and reconciling accounts. They should implement tools and controls to plug their biggest leaks.

### **Credit Card Fraud**

Credit cards are the most widely accepted modes of payment, and their channels for payment are also varied. With the growth of the Internet, credit cards have become the dominant form of online payments. Not surprisingly, companies lost more money from credit card fraud, than through any other payment method.

Though there has been a steady decline in losses in proportion of sales, the volume of losses has actually increased. This is driven, in large part, due to the ubiquity of the Internet and the relative ease with which a payment could be made online.

### **Debit Card Fraud**

With the growing popularity of debit cards in the last few years, institutions have moved in with newer offerings in the form of signature cards. While PIN debit cards were fairly safe, the signature debit cards are

extremely vulnerable to fraud. The primary reason for this is the lack of diligence of merchants to verify signatures. Debit card fraud, in general, is on the rise because of sophistication in the tools available at the fraudsters' disposal and improvement in real-time credit card detection technologies, which has forced perpetrators to the world of debit cards.

Compared to checks and ACH, debit cards have a higher proportion of loss relative to the size of the market. With improved technology playing a part in reducing credit card fraud, it is only prudent that firms adopt the same tools to minimize debit card fraud. Firms should opt for systems that cover both signature and PIN debit cards.

Since most financial services firms maintain discretion on the subject of fraud, these numbers may well be underestimated. Statistics also vary across sources due to differences in approach and lack of data. Nonetheless, they still tell a consistent story. Losses from fraud are

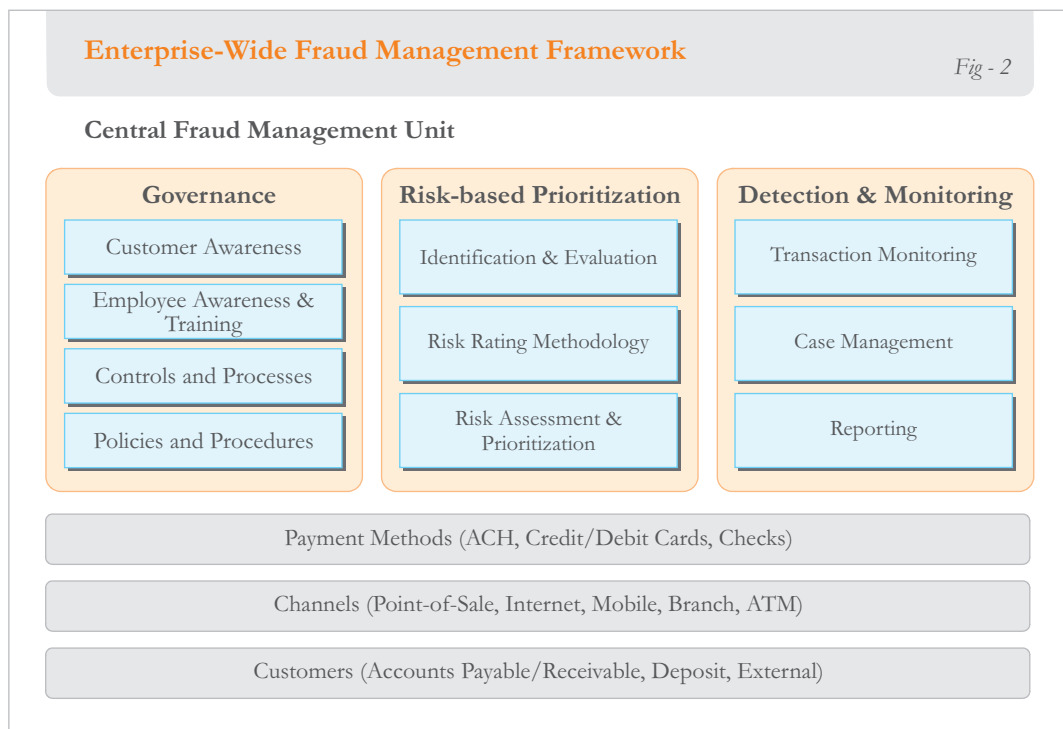
mounting and financial services firms need to be on their toes more cautiously than before.

### Preparing for the Fight

The fight against fraud can't be won with a disjointed army. While most firms have various tools and processes in place, these are disjointed and they operate in silos. Fraudsters take advantage of this lack of integration between organizational silos to maneuver between channels while committing fraud. It's important that firms look at fraud holistically across the entire enterprise to have a better chance at catching such activities. Such a framework can help firms counter fraud, using a consistent and disciplined approach across the entire organization.

Based on experience, working with clients that have been successful in tackling fraud, we believe an enterprise-wide framework should have the following components:

- *Centralized Fraud Management Unit* to



formulate the overall anti-fraud strategy and to establish direction

- *Risk-based Prioritization* framework to evaluate the relative risk of fraud across business lines, products, channels, and customers and to prioritize anti-fraud projects accordingly
- *Governance* mechanism to establish standardized policies, procedures and controls
- *Tools and Systems* to detect, monitor and report fraud

### **Establishing the Command - Centralized Fraud Management Unit**

Over the past few years, firms have started looking at risk management across the entire enterprise which is a departure from silo-based approaches. This integration across business lines, products, accounts, and functions is gradually gaining ground in some of the more traditional areas of operational, credit and market risk. Companies have formed enterprise risk management committees to set the strategy and provide direction and oversight. However, except for a few of the leading financial services firms, we haven't seen such action in the fraud space. Dealing with fraud continues to be a business line responsibility, with very little interaction between different groups. Companies would do well to establish a centralized fraud management unit to drive the anti-fraud agenda and set the direction. Without this central command, it will be very difficult for firms operating in silos to achieve the level of integration required to combat fraud comprehensively.

From an operational perspective, this central unit could be part of the enterprise risk management committee. This would not only make fraud an integral component of

operational risk management, but also ensure consistency in risk measurement, prioritization and mitigation. This unit will be responsible for laying down the fraud strategy and objectives, and defining the framework components and implementation strategy. Appropriate responsibility will be delegated to this unit to establish risk ownership and drive participation across the enterprise.

### **Choosing the Battles: Risk-based Prioritization Framework**

As the payments landscape has evolved, so have the ways in which fraudsters can defraud. Given budget constraints, a financial services firm will have to choose its battles and the appropriate tools to fight them. A risk-based prioritization of the payment methods in use can help identify and select the tools most appropriate for the battle.

Firms often adopt a one-size-fits-all approach for fraud detection and monitoring, without taking into account differences between products and services, customers, payment methods and channels. A clear understanding of these areas and the ways and means in which frauds are executed can help draw a roadmap for implementing the right tools and controls.

The first step is to identify the different payment processes at work and collect relevant fraud metrics across products, delivery channels, and customer segments to evaluate their relative risk. These metrics should include both qualitative and quantitative measures to determine the following:

- How vulnerable a payment method is to fraud (number of attacks, likelihood of attack, dollar value of attempted attacks, strength of internal and external controls, sophistication of monitoring and detection, etc)
- Loss from fraud (dollars lost, dollars lost per

incident, dollars lost per \$100 of transaction, operational cost of remediation, etc)

Each payment area is assigned a risk rating based on quantitative and qualitative metrics. Based on the risk rating, high risk areas should be identified for further analysis. Key controls and monitoring systems in the high risk areas can be assessed and remedial action can be taken to further improve or strengthen them.

### Getting Ready for Combat: Governance

Most financial firms have multiple business lines catering to different products and customer bases across multiple geographies. It is often difficult to get a consolidated view of all the fraud management practices across this maze. In this environment, it is imperative that firms adopt strong governance practices to enforce standardized policies, procedures and controls across the entire organization.

Several key dimensions need to be considered in establishing a governance framework.

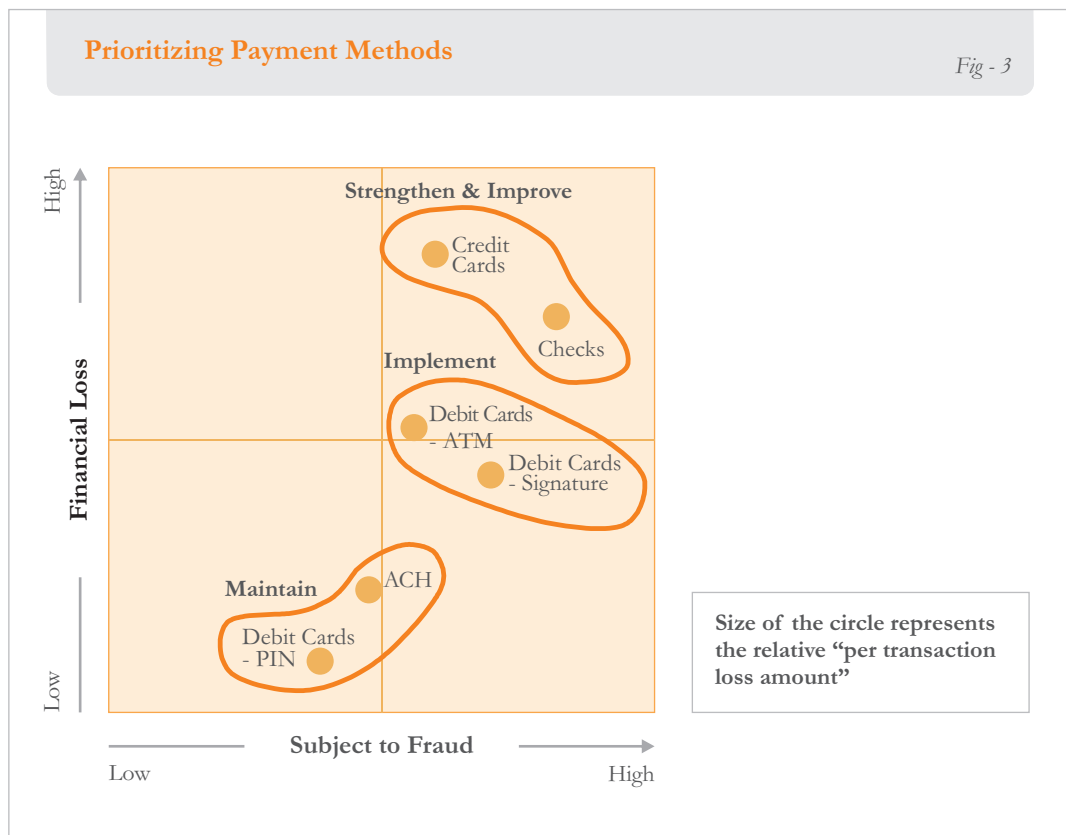
### Customer Awareness

Fraudsters target customers by taking advantage of specific channels and payment behaviors. It is important that firms work closely with customers in educating them about mechanisms to prevent fraud. Such initiatives could go a long way in preventing fraud and saving detection and investigation costs.

It is not only important to adopt these initiatives, but it is also critical to understand the effectiveness and impact these initiatives have in preventing fraud.

### Employee Monitoring and Awareness

Employees can collude with external fraudsters or interact with other employees in different departments to either access sensitive client information, or use information to



defraud the company. Employees need to be monitored constantly to ensure that they are not misusing information to their advantage.

Training also plays a key part in educating employees about different kinds of frauds and how these are proliferated. Firms should build training programs and constantly update and enhance them to keep up to the changing market trends.

### **Controls, Policies and Procedures**

Based on many industry surveys, it has been observed that one of the primary reasons for the high incidence of fraud is “failure to implement fraud prevention services”. Most often, this is due to a lack of awareness of the services and unwillingness to bear the cost of adding additional services. Firms have to ensure that fraud prevention controls like positive pay, reverse pay and ACH debit blocks are incorporated across the payment systems.

As companies introduce new products into the market, it's important for them to map the associated business processes, internal and external touch points to payment systems. Moreover, a thorough assessment of controls for each channel of payment for the product needs to be carried out. Cross-channel and multi-product business processes will need a more granular assessment to identify potential ways to circumvent the controls.

A key control element is the delineation of responsibilities. Payment processes need to be reviewed to ensure an adequate level of separation between processes that can be misused. For example, origination, approval and reconciliation need to be separated from each other. Key processes like reconciliations should be carried out under strict SLAs and breaks should be fixed to prevent errors.

With a constantly evolving payments landscape and integration of newer channels,

it has become important to ensure that policies and procedures are constantly updated. Additionally, processes need to be introduced to study industry best practices and recommendations, and incorporated into relevant firm-wide policies and procedures.

### **Arming for the Fight: Detection, Monitoring, and Reporting Systems**

A key component of the payments fraud framework is detection and monitoring. Different payment methods have different characteristics and need different approaches to identify fraud. There are dedicated solutions to monitor fraud of credit cards, debit cards, ATM, ACH and wires. Techniques to monitor fraud in each of these payment methods have also evolved considerably over the last few years. For example, use of predictive analytic models, neural networks and improved profiling has reduced the basis points lost to fraud, while bringing down the number of exceptions. The ability to block fraudulent transactions in-flight is also becoming integral to detection and monitoring. The adoption of real-time payment screening methods, driven partly by industry initiatives to shorten the payment lifecycle, is also helping reduce the overload of after-the-fact exceptions.

While it would be naïve to think of having a single system for monitoring all payment methods, there is a clear need to integrate systems across methods and channels to obtain a single view of the customer. For example, ACH and check payment systems need to communicate with each other if they are to catch a fraudulent check, caught by positive pay from being presented as an ACH debit. Detection systems also need to be tied closely to KYC and account opening systems to ensure that key customer information is factored into the monitoring process. A single

view of the customer across all accounts, payment methods and channels is required to identify cross-channel fraud and to evaluate the real risk. A key trend that we are observing in this integration process is the emergence of case management. This ability to connect the dots and paint a broader picture, aided by a single case management system is becoming increasingly important in an interconnected world where payments methods and channels interact seamlessly.

Another key weapon in this fight against fraud is the ability to collate and present relevant fraud information to senior management. Being able to aggregate and report fraud metrics and report can help the senior management to better understand and prioritize risks.

### Real-time Payment Screening

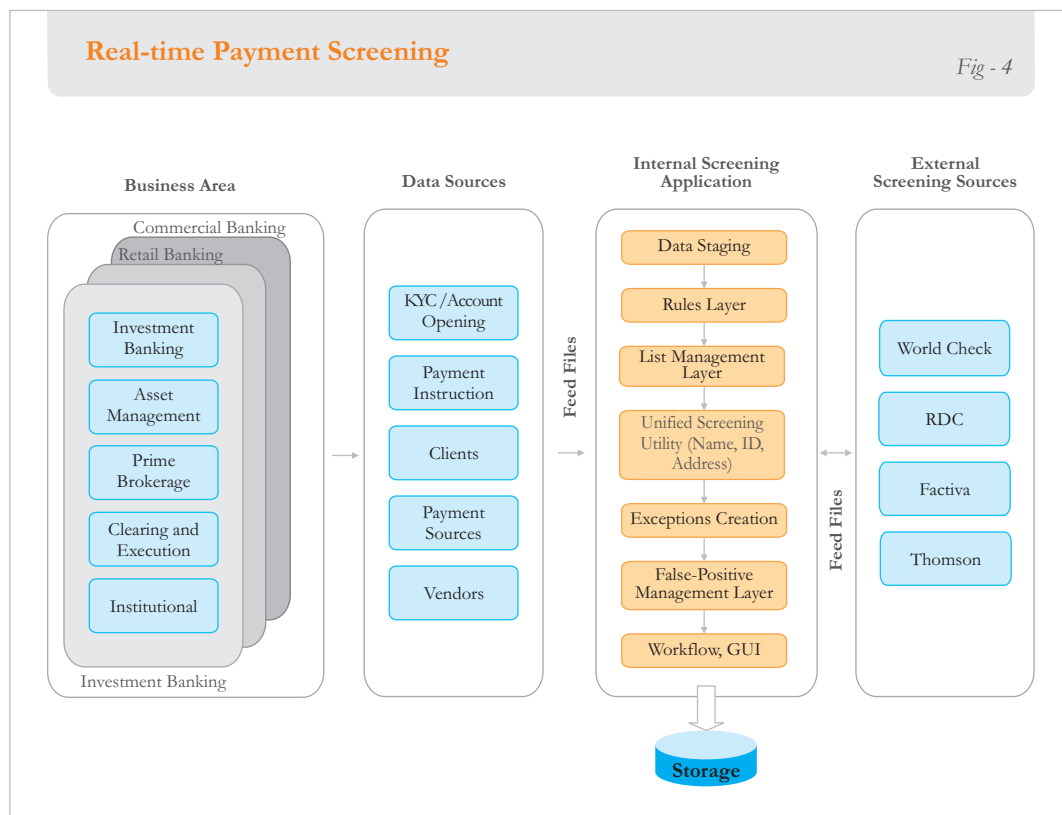
While after-the-fact detection is an effective

tool in countering fraud, firms will be able to realize maximum benefit by investing in real-time screening applications that isolate potentially fraudulent transactions in-flight. Real-time screening of payments not only helps reduce false positives and the operational cost associated with it, but also quickens the remediation process.

Firms should adopt a unified approach of screening, where different business lines route information to a centralized screening utility that manages the entire screening lifecycle. This central utility obviates the need for multiple hookups to external screening utilities, thereby reducing costs.

### Case Management

Recent studies show that enterprise case management is one of the top priorities for financial services firms in their fight against fraud. Firms should direct greater resources



towards ensuring tighter integration of case management systems with detection platforms. With a case management system, analysts won't have to comb through multiple monitoring systems during the investigation process. With information aggregated from multiple systems, it becomes much easier to detect patterns of unusual behavior and build a case against fraud.

A good case management system should have the ability to normalize data from different payment monitoring systems and link them to form cases. It should provide functionality to interface with external vendors and government agencies to share information. Moreover, it should have interfaces with senior management risk and compliance dashboards, besides supporting reporting and querying.

### **Metrics and Reporting**

The senior management's ability to evaluate the risk of fraud across products and payment methods, and to prioritize anti-fraud measures depends on data. Dashboards to provide metrics such as fraud rates, loss basis points, reduction in false positives, chargebacks, etc. can empower senior managers to take more informed decisions.

Some of these key metrics include:

- Dollars lost to fraud, fraud loss as a percentage of revenues, dollars lost per incident, ratio of number of incidents with losses to total number of attacks
- List of fraud projects (by business line, product, channel and customer segment), investments, hit rates, false positive rates
- Business processes with level of fraud risk, associated controls, high level summary of evidence to prove the existence of controls
- Employee profiles (e.g., top 10th percentile in all the different categories of risk levels associated with employees)
- Mapping of training programs to regulations, number of employees trained/re-trained, number of customer surveys and trainings conducted

As new payment methods and channels evolve, there will be a corresponding rise in frauds across them. Firms will be able to better position themselves to manage the risk of fraud by adopting an enterprise-wide fraud management framework that focuses on integration, governance and monitoring. A robust governance and risk-prioritization framework with adequate focus on tools like real-time payment monitoring and case management can significantly bring down false positive and fraud rates.



### **Debashis Pradhan**

*Principal Consultant  
Infosys Consulting*

*Debashis is a Principal Consultant with the Banking & Capital Markets Group at Infosys Consulting. He has close to 7 years of professional experience collaborating with clients to develop and implement complex business transformational programs. His areas of focus include Regulatory Compliance, Operational Effectiveness, Data Strategy, and IT-enabled Business Solutions.*



### **Naveen Balawat**

*Senior Associate  
Infosys Consulting*

*Naveen is a Senior Associate with the Banking & Capital Markets Group at Infosys Consulting. He has more than 7 years of experience in the financial services industry. His areas of focus include Private Wealth Management, Middle Office, Regulatory Compliance, Insider Monitoring, and AML.*

*The authors would like to thank Parikshit Chondbary and Rajat Gurnani for their contributions to this article. Parikshit and Rajat are Business Analysts with the Banking & Capital Markets Group at Infosys.*



POWERED BY INTELLECT  
DRIVEN BY VALUES

For information on obtaining additional copies, reprinting or translating articles and all other correspondence, please email: [bcm@infosys.com](mailto:bcm@infosys.com)

## GLOBAL PRESENCE

### North America

Atlanta, Bellevue, Bridgewater, Charlotte, Detroit, Fremont, Houston, Lake Forest, Lisle, Mexico, New York, Phoenix, Plano, Quincy, Reston, Toronto

### Europe

Brussels, Copenhagen, Frankfurt, Geneva, Helsinki, London, Milano, Oslo, Paris, Stockholm, Stuttgart, Utrecht, Zurich

### Asia Pacific

Beijing, Hongkong, Mauritius, Melbourne, Shanghai, Sharjah, Sydney, Tokyo

### India

Bangalore, Bhubaneswar, Chandigarh, Chennai, Gurgaon, Hyderabad, Jaipur, Mangalore, Mumbai, Mysore, New Delhi, Pune, Thiruvananthapuram

## ABOUT INFOSYS

Infosys Technologies Ltd. (NASDAQ: INFY) defines, designs and delivers IT-enabled business solutions that help Global 2000 companies win in a Flat World. These solutions focus on providing strategic differentiation and operational superiority to clients. Infosys creates these solutions for its clients by leveraging its domain and business expertise along with a complete range of services. With Infosys, clients are assured of a transparent business partner, world-class processes, speed of execution and the power to stretch their IT budget by leveraging the Global Delivery Model that Infosys pioneered.

For more information,  
contact: [bcm@infosys.com](mailto:bcm@infosys.com)

[www.infosys.com](http://www.infosys.com)

2008 Infosys Technologies Limited, Bangalore, India. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document.