Infosys™ McCamish

ANALYSIS OF INFOSYS MCCAMISH SYSTEM OUTAGE 2023

MSIS 523 Presentation - TEAM 04

Kelly, Peifen, Rish, Shalaka, Tony

TABLE OF CONTENTS

THREAT LANDSCAPE

22+

Years of experience

750

associates on platform

34

customers

680+

employees

6

awards

CUSTOMERS

- 34 Long-term clients including 7 of the top 10 US insurers.
- 10+ PMACS clients in the US and Canada
- 28 VPAS PAS and PMACS clients

SERVICES

SOLUTIONS - life insurance and annuity services, including employer-sponsored plans, retirement services, and functional BPO solutions.

PLATFORMS - Infosys McCamish NGIN, PMACS Platform, STEP Platform, VPAS Platform, and VPAS BPA

ASSETS

APPLICATIONS & SERVICES:

- Availability
- Confidentiality
- Integrity

PII DATA:

- Confidentiality
- Regulation Compliance
- Integrity

CYBERSECURITY POSTURE

Cybersecurity Risk Assessment Framework

Design:

- Early engagement
- Compliance focus
- Robust security architecture

Scale:

- Cost optimization
- Rapid development
- Integrated security solutions

Future:

- Innovation emphasis
- Collaboration
- Ongoing competency building

Compliance

ISO 14001
ISO 22301
ISO 27001
ISO 27701
ISO 45001

Approach & Strategy

1. transparency & experience
2. continual improvement & compliance
3. cyber resilience
4. building & maintaining a positive cyber security culture within the organization.

Partnerships

Engaged since May 2022 with Palo Alto Networks Inc.’s Unit 42 to strengthen customer’s security posture for secure digital transformation.

Services - cloud delivered security platform to assure security - network perimeters, workloads & workplace, cloud, and secured access.

THE INCIDENT

Nov 2, 2023

Infosys McCamish System (IMS) Outage detected resulting in unavailability of certain applications and systems. Customers temporarily suspended contract transactions, including:

- beneficiary changes
- cash withdrawals
- death claim payments

Nov 15, 2023

IMS Outage persists. There is no indication that client data is impacted. Recordkeepers resort to filing paper forms via phone or by physical mail.

Nov 24, 2023

IMS Outage persists. Bank of America deferred compensation plan customers' information was possibly compromised.

Dec 8, 2023

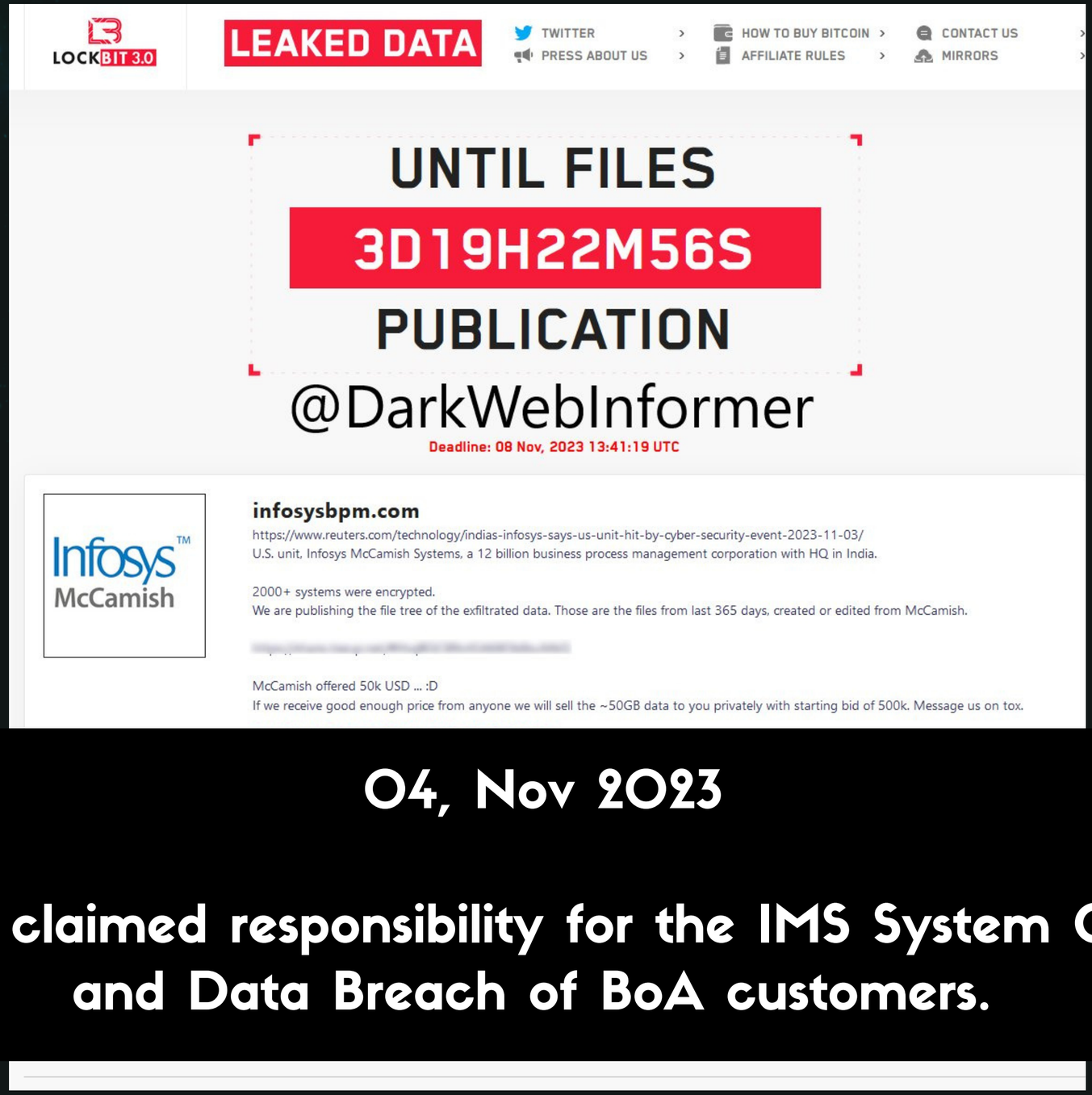
IMS back online; contract transaction processing restored.
Delay expected in full restoration of online services because:

- Recordkeepers will validate the safety and security of restored IMS systems.
- Backlog of 1 month of transactions.

Dec 31, 2023

IMS fully restored and all Recordkeepers resumed normal operations.

THE RESPONSIBLE



04, Nov 2023

LockBit claimed responsibility for the IMS System Outage and Data Breach of BoA customers.

WHO IS LOCKBIT

- Top ransomware family - pervasiveness recognized by CISA, FBI, and other international security bureaus.
- One in every six ransomware attacks targeting US government offices in 2022 was attributed to LockBit.

example, last year, the Cybersecurity & Infrastructure Security Agency in conjunction with other U.S. Departments and Agencies and foreign partners published two cybersecurity advisories, "Understanding Ransomware Threat Actors: LockBit" and "LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability." These advisories detail the threats posed by this group and provide recommendations to reduce the likelihood and impact of future ransomware incidents.

U.S. Treasury Designates Russian State-Owned Sovcomflot, Russia's Largest

- Ransomware-as-a-Service (RaaS) model that operates through three phases:
  - exploitation
  - infiltration
  - deployment
- Fast encryption speeds
- Spreads via: Remote Desktop Protocol (RDP) exploitation, phishing campaigns, and abuse of valid accounts.

MITIGATION AND RECOVERY EFFORTS

WHAT DID INFOSYS DO?

- Rapid Response:
  - Partnered with Palo Alto Networks' Unit 42
- Restoration and Hardening of Systems:
  - patching vulnerabilities and implementing stronger security measures

WHAT DID INFOSYS DO?

- Communication:
  - All stakeholders informed within hours of the incident
  - BSE Ltd., National Stock Exchange of India Ltd., New York Stock Exchange and to United States Securities and Exchange Commission on November 3, 2023.

- As of Feb 26, 2024 - no knowledge of ransom being paid to lockbit

Infosys
Navigate your next

TO ALL STOCK EXCHANGES

BSE LIMITED
NATIONAL STOCK EXCHANGE OF INDIA LIMITED
NEW YORK STOCK EXCHANGE

November 3, 2023

Dear Sir, Madam,

Sub: Company Statement

Infosys McCamish Systems ("IMS"), a subsidiary of Infosys BPM Limited (a wholly owned subsidiary of Infosys Limited) has become aware of a cybersecurity event resulting in non-availability of certain applications and systems in IMS.

Data protection and cybersecurity are of utmost importance to us. We are working with a leading cybersecurity products provider to resolve this at the earliest and have also launched an independent investigation with them to identify potential impact on systems and data.

This is for your information and records.

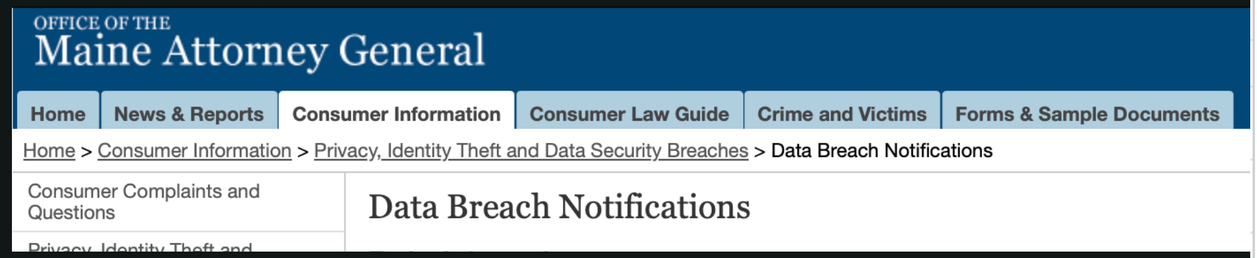
Yours sincerely,
For **Infosys Limited**

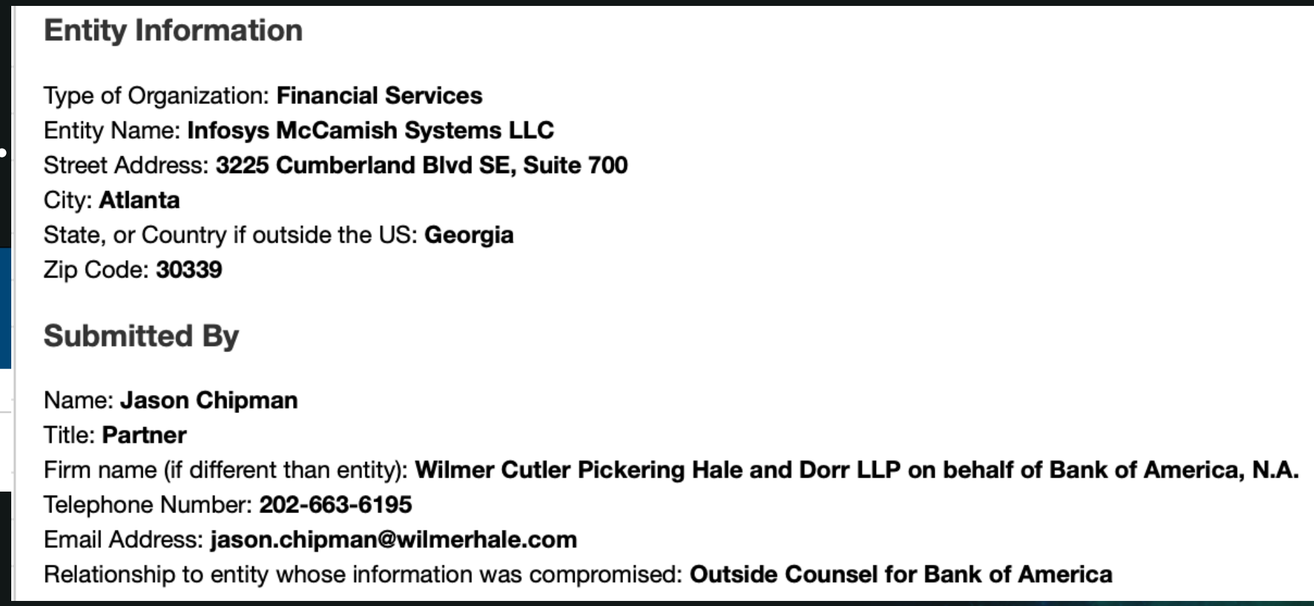
SURYANARAYANA ANUR GURUGOPALA RAJU MANIKANTHA
Digitally signed by SURYANARAYANA ANUR GURUGOPALA RAJU MANIKANTHA
Date: 2023.11.03 15:47:55 +05'30'

A.G.S. Manikantha
Company Secretary

THE AFTERMATH

- Disruption of business activities and Data Breach of 57028 BoA customers.
- BoA offered a complimentary 2-yr membership in Experian IdentityWorks for eligible affected customers, which includes:
  - Identity detection services.
  - Daily monitoring of credit reports from Experian, Equifax®, and TransUnion®.
  - Internet surveillance.
  - Resolution of identity theft issues.





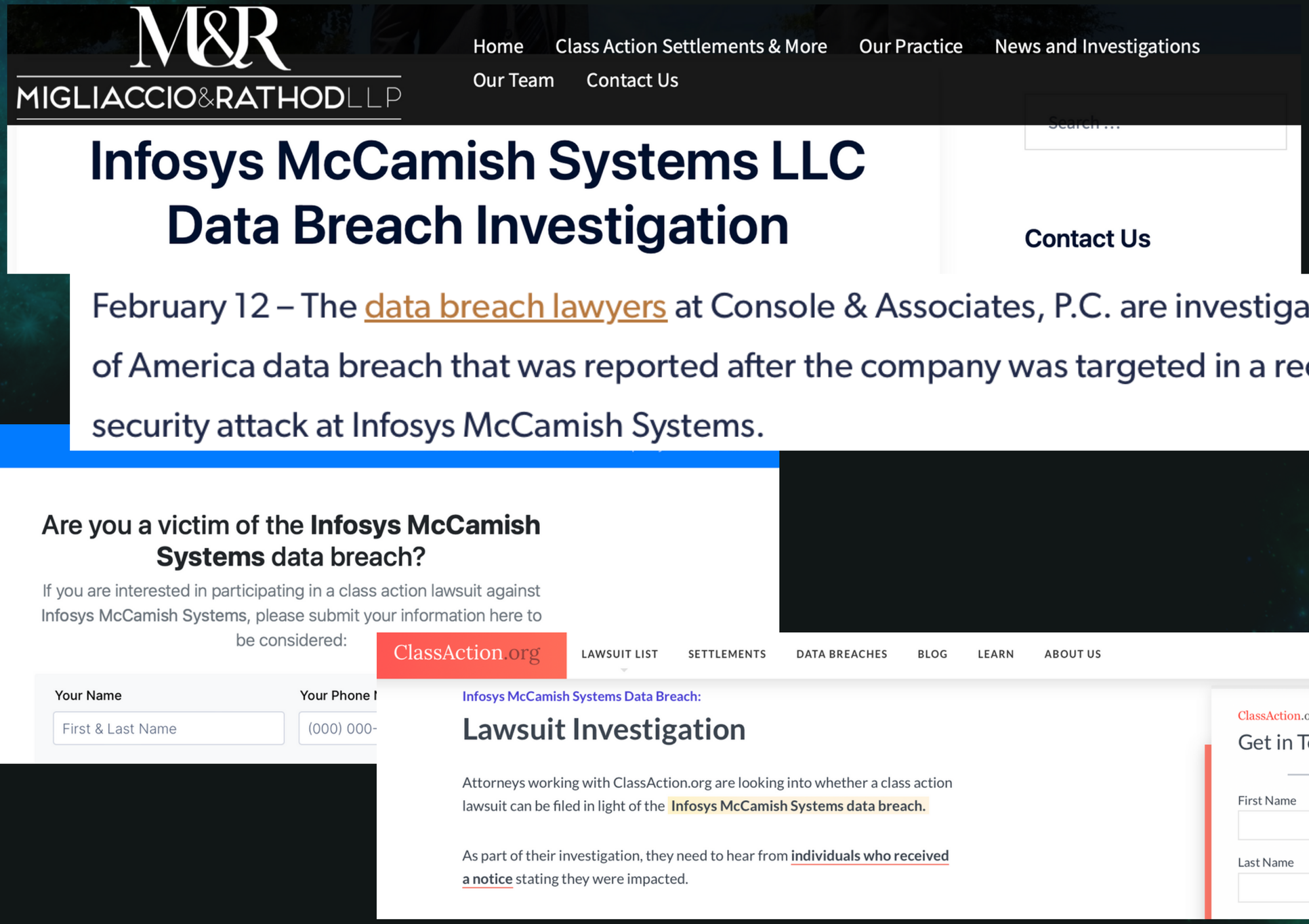
Entity Information

Type of Organization: **Financial Services**
Entity Name: **Infosys McCamish Systems LLC**
Street Address: **3225 Cumberland Blvd SE, Suite 700**
City: **Atlanta**
State, or Country if outside the US: **Georgia**
Zip Code: **30339**

Submitted By

Name: **Jason Chipman**
Title: **Partner**
Firm name (if different than entity): **Wilmer Cutler Pickering Hale and Dorr LLP on behalf of Bank of America, N.A.**
Telephone Number: **202-663-6195**
Email Address: **jason.chipman@wilmerhale.com**
Relationship to entity whose information was compromised: **Outside Counsel for Bank of America**

- As of Feb 26th, 2024, no reports of identity theft related to the breached data have been reported.
- Cost of Incident to Infosys: **US $30 million (approx.) vs. avg US$ 4.45 million**



M&R
MIGLIACCIO&RATHODLLP

Home Class Action Settlements & More Our Practice News and Investigations
Our Team Contact Us

Search ...

Infosys McCamish Systems LLC Data Breach Investigation

Contact Us

February 12 – The data breach lawyers at Console & Associates, P.C. are investigating the Bank of America data breach that was reported after the company was targeted in a recent cyber security attack at Infosys McCamish Systems.

Abington Cole + Ellery

Are you a victim of the **Infosys McCamish Systems** data breach?

If you are interested in participating in a class action lawsuit against Infosys McCamish Systems, please submit your information here to be considered:

Your Name

First & Last Name

Your Phone

(000) 000-

ClassAction.org

LAWSUIT LIST SETTLEMENTS DATA BREACHES BLOG LEARN ABOUT US

Search lawsuits, settle

Infosys McCamish Systems Data Breach:

Lawsuit Investigation

Attorneys working with ClassAction.org are looking into whether a class action lawsuit can be filed in light of the **Infosys McCamish Systems data breach.**

As part of their investigation, they need to hear from **individuals who received a notice** stating they were impacted.

ClassAction.org

Get in Touch

First Name

Last Name

CONCLUSION

CONCLUSION

- “It is unlikely that we will be able to determine with certainty what personal information was accessed as a result of this incident.”

  - Infosys

- Annual report 2022 vs 2023
  - Added data protection and privacy
  - Risk management framework remains the same

STEPS OF A GOOD RISK MANAGEMENT PLAN

- Identify Assets
  - Sensitive Data
  - Payment Data
- Identify Threats
- Identify Vulnerabilities
- Determine Risk Tolerance
  - Low tolerance because of the industry
- Implement Safeguards and Controls

Questions & Comments

Keep your data close

and your vendors closer.

FLOW.

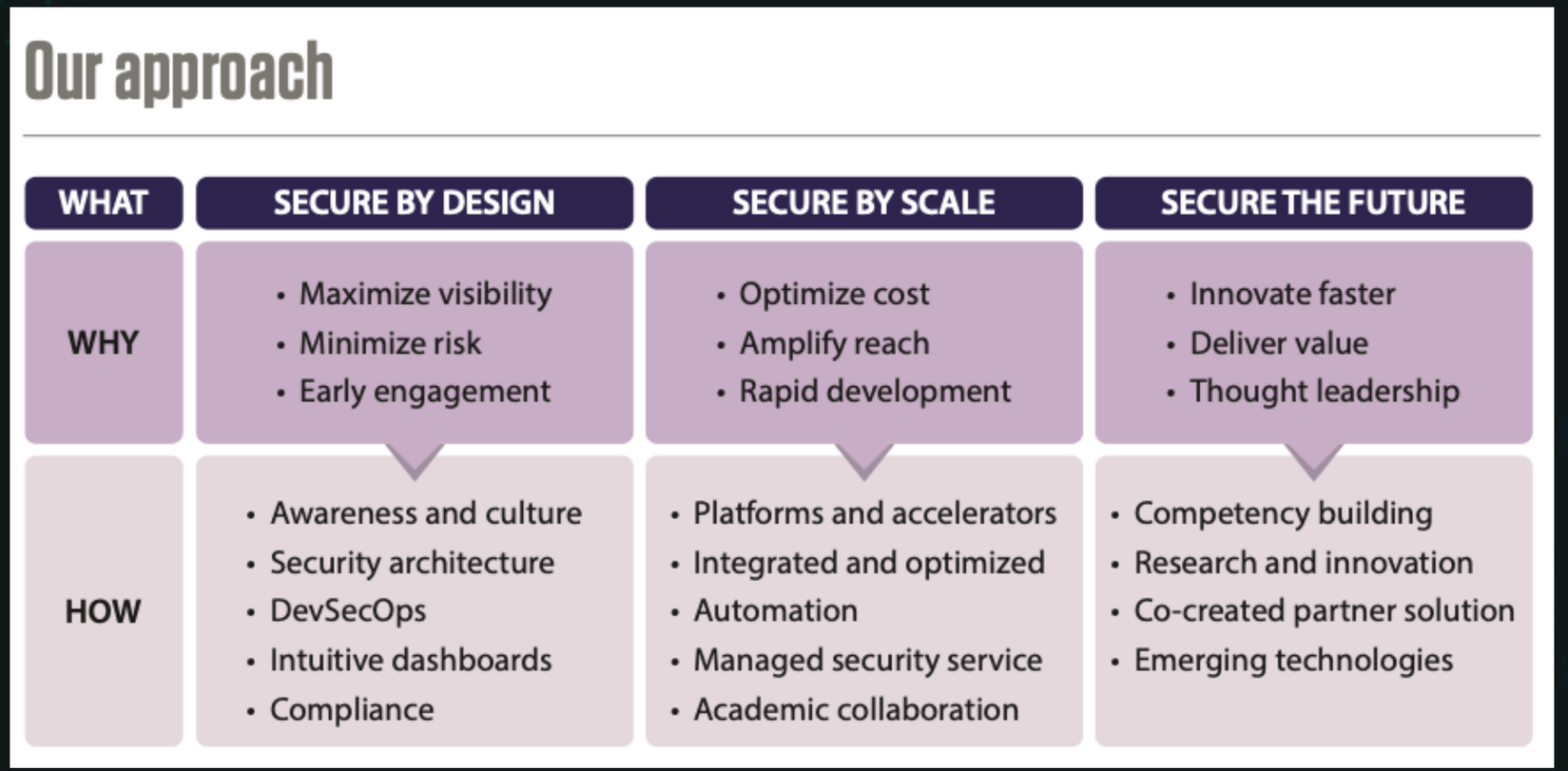
APPENDIX

1. Infosys Information Management

Link: https://www.infosys.com/sustainability/documents/esg-2022-23/gov-story6.pdf

2. **Infosys McCamish System**

Link: https://www.infosysbpm.com/mccamish.html



APPENDIX

3. Infosys McCamish Customers Suspend Transactions

Link to News Article: https://apps.web.maine.gov/online/aeviewer/ME/40/c2da936e-14f0-421a-833e-a24cbdd79cfa.shtml

"At this time, there is no indication that client data is impacted," TIAA's spokesperson said. "[W]e are working with the impacted vendor to restore operations as soon as possible … [W]e are unable to provide an estimated timeline for resolution."
As a result of the issue at Infosys McCamish Systems, TIAA Life temporarily suspended certain contract transactions, including beneficiary changes, cash withdrawals, death claim payments, dollar-cost averaging, investment allocation changes, premium payments, rebalancing and systematic withdrawals, the firm disclosed.

4. Infosys Ransomware Breach Resolving, but Accounts Still Down

Link: https://www.plansponsor.com/infosys-ransomware-breach-resolving-but-accounts-still-down/

5. U.S. Cybersecurity and Infrastructure Security Agency Advisory for Lockbit

Link: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

Cyber Incident at Infosys Unit Hits TIAA Annuity Services

Three TIAA retail, after-tax deferred variable annuities are among the products affected by the incident at Infosys McCamish Systems, TIAA disclosed Monday.

By Beagan Wilcox Volz | November 15, 2023

A "cyber security event" at a vendor for some of **TIAA Life**'s variable annuity and variable life insurance products has left contract owners and policy holders unable to access many services, the firm disclosed Monday in a regulatory filing.

Infosys McCamish Systems "is currently experiencing an outage" because of the cyber incident, a TIAA spokesperson said.

"At this time, there is no indication that client data is impacted," TIAA's spokesperson said. "[W]e are working with the impacted vendor to restore operations as soon as possible … [W]e are unable to provide an estimated timeline for resolution."

As a result of the issue at Infosys McCamish Systems, TIAA Life temporarily suspended certain contract transactions, including beneficiary changes, cash withdrawals, death claim payments, dollar-cost averaging, investment allocation changes, premium payments, rebalancing and systematic withdrawals, the firm disclosed.

Online services aren't available, according to TIAA Life's disclosure.

APPENDIX

6. Company Communication to SEC and Stock Exchanges:

Link: https://www.infosys.com/investors/documents/company-statement-3nov2023.pdf

7. Excerpt from the letter addressed to the stock exchange following the Board meeting convened on January 10-11, 2024:

Link: https://www.infosys.com/investors/documents/outcome-board-meeting-11jan2024.pdf

2.6.2 McCamish cybersecurity incident
In November 2023, Infosys McCamish Systems (McCamish) a step down subsidiary of Infosys Limited experienced a cybersecurity incident resulting in the non-availability of certain applications and systems. McCamish initiated its incident response and engaged cybersecurity and other specialists to assist in its investigation of and response to the incident and remediation and restoration of impacted applications and systems. By December 31, 2023, McCamish, with external specialists' assistance, substantially remediated and restored the affected applications and systems.
Loss of contracted revenues and costs incurred with respect to remediations, restoration, communication efforts and others amounted to approximately **$30 million**.

Infosys had previously communicated the occurence of this cybersecurity incident to BSE Limited, National Stock Exchange of India Limited, New York Stock Exchange and to United States Securities and Exchange Commission on **November 3, 2023**.

APPENDIX

7. Data Breach Notification submitted to Maine State Government:

Link to Notification: https://apps.web.maine.gov/online/aeviewer/ME/40/c2da936e-14f0-421a-833e-a24cbdd79cfa.shtml

Bank of America is offering a complimentary two-year membership in an identity theft protection service provided by Experian IdentityWorks for eligible affected customers. This product includes identity detection which includes daily monitoring of an individual's credit reports from the three national credit reporting companies (Experian, Equifax® and TransUnion®), internet surveillance, and resolution of identity theft. This service will expire at the conclusion of the complimentary period and will not automatically renew.

8. Service Update for Vanguard Nonqualified Plan Sponsors

Link: https://si-interactive.s3.amazonaws.com/prod/plansponsor-com/wp-content/uploads/2023/11/16212819/11.16.2023-Vanguard-NQP-Service-Update-Nov-16.pdf

9. Infosys Integrated Annual Reports

2022 Report Link: https://www.infosys.com/investors/reports-filings/annual-report/annual/documents/infosys-ar-22.pdf

2023 Report Link: https://www.infosys.com/investors/reports-filings/annual-report/annual/documents/infosys-ar-23.pdf

APPENDIX

Risks Identified in 2022 Report

Key risks	Mitigation approach
Adverse geo-political, economic or health events may impact demand for our offerings and /or technology and talent supply chain.	Broad-based growth to reduce concentration in any single region, client or industry, operational agility to assess and respond to situations
Commoditization of traditional offerings may impact our market share and profitability.	Investment in launching innovative new offerings, a broad portfolio of interconnected services and solutions, and focused growth of digital capabilities
Talent attrition beyond acceptable levels may impact our ability to staff projects or optimize cost structures.	Employee engagement and care, holistic employee retention and recognition policies, focus on career and leadership development
Cost inflation may impact our cost structure and longer-term profitability.	Effective operations with sustainable cost optimization levers, automation and planned capex program
Disruptive technologies such as cloud, software-as-a-service and automation software may diminish the value of some of our service offerings (emerging risk).	Robust alliance strategy, consulting and industry-domain-knowledge-led solutions, reskilling program for employees into newer technologies and methodologies, and large deal program
Cyber attacks that breach our information network or failure to protect sensitive information of our stakeholders in accordance with applicable laws may impact our operations or result in significant regulatory penalties.	Robust cybersecurity framework, controls, governance, preparedness for response to incidents, insurance, region-specific data protection controls and awareness campaigns
New regulations or amendments to existing regulations (e.g., immigration, wages, tax, sanctions) may have an adverse impact on our operations (emerging risk).	Active engagement with policymakers and trade associations, well-governed compliance framework and controls, and de-risked operations
If our employees operate remotely for extended periods, it may adversely impact their productivity, our information security controls and the social capital of the organization.	Implement a hybrid operational model that balances client requirements, evolving employee preferences, legal requirements and information security risks
Physical disasters or climate change events may adversely impact our operations.	Well-established and tested business continuity plans, crisis management policy, distributed operations, sustainability and community engagement initiatives

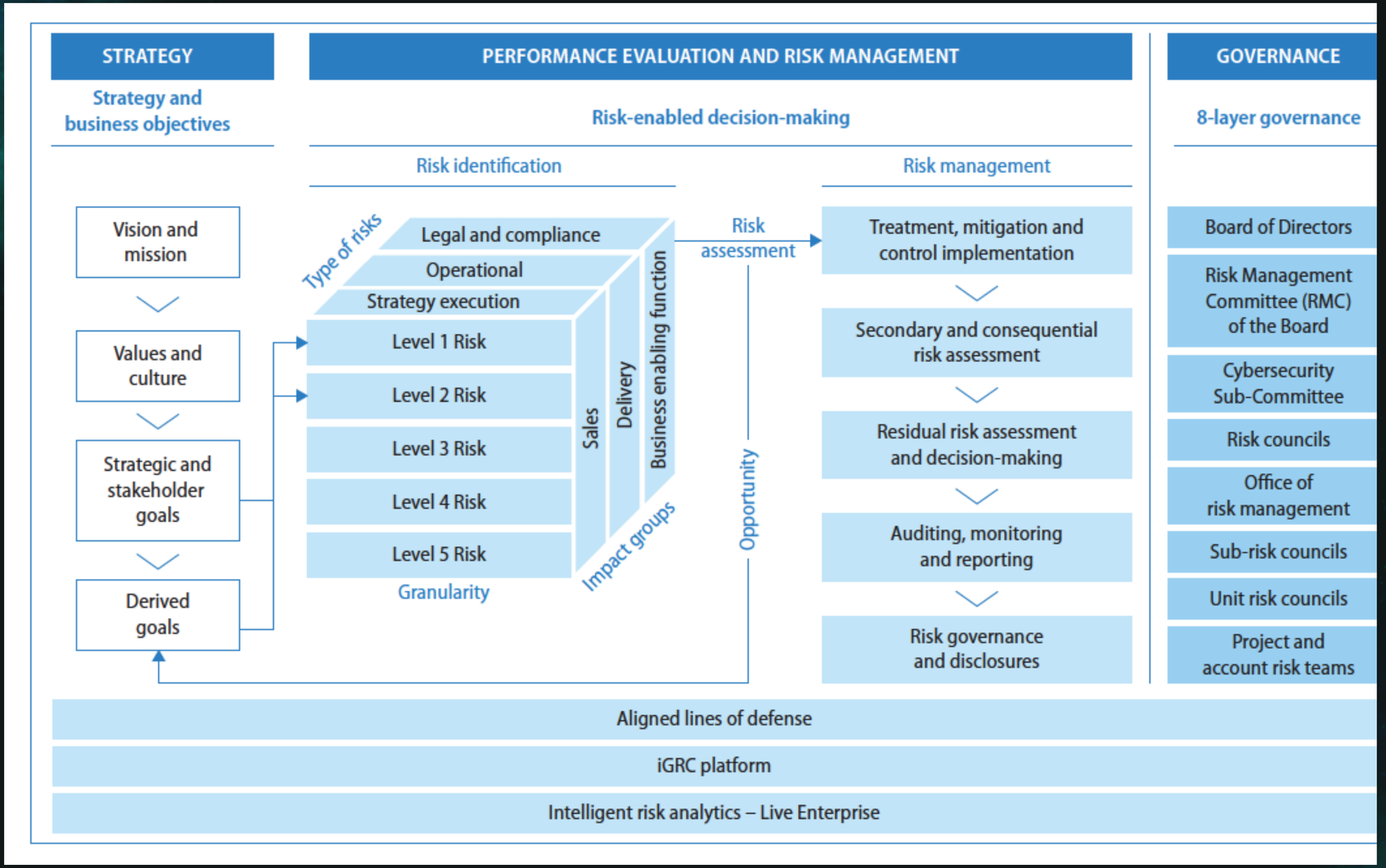
APPENDIX

Risks Identified in 2023 Report

Key / Emerging risks	Impact on Company	Mitigation / Opportunity
Geo-political, macro-economic or health events	• Unfavorable geo-political, economic or health events may result in currency volatility and reduced spend on technology products and services which may adversely impact demand for our offerings which in turn may impact our growth and profitability. • **Emerging risk aspect:** Geo-political, economic or health events are dynamic in nature and constantly evolving. Uncertainty about new changes therefore sometimes makes it difficult to predict and assess the impact. • **Impacted capitals:** Financial, Social & Relationship and Human	• Broad-based growth to reduce concentration in any single region, client or industry • Operational agility to assess and respond to situations, including enablement of remote working, working out of multiple DCs / locations, etc. • Currency hedging • **Opportunity** – Clients are looking for IT projects which can help them take out costs.
Commoditization of services and heightened competitive landscape	• If we are unable to differentiate our offerings and manage customer expectations in times of intense competition in the market for technology services, this could affect our win rates and pricing, reduce our market share and decrease our revenue and profits. • **Impacted capitals:** Financial and Intellectual	• Differentiation though innovation and industry solutions • Increased automation • Investment in launching innovative new offerings • A broad portfolio of interconnected services and solutions • Focused growth of digital capabilities
Technology disruption and innovation	• **Emerging risk:** Not having the right framework and approach to identify, invest in, incubate and operationalize new services and offerings that are in line with technology changes, client preferences and market expectations may disrupt our value proposition and reduce our relevance to customers, impacting our revenue and profitability. The speed and nature of technological changes make it difficult to predict the trend. • **Impacted capitals:** Financial, Human and Intellectual	• Innovation framework • Investments in research and development • Robust alliance strategy • Consulting and industry / domain knowledge led solutions • Reskilling program for employees into newer technologies and methodologies • Large deal program • **Opportunity** – Identify, develop and deploy new offerings to customers leveraging next-generation technologies.
Talent supply constraints and Hybrid working model	• If we are unable to hire, engage and retain technology and management talent, manage leadership succession and transition, respect and protect human rights, continuously evolve our hybrid work model in response to changing needs and expectations, it could impact our reputation, ability to staff projects or execute large and complex programs, or optimize cost structures. • **Impacted capitals:** Financial, Human and Intellectual	• Employee engagement and support • Holistic employee retention and recognition efforts • Focus on career and leadership development • Hybrid operational model that balances client requirements, evolving employee preferences, legal requirements and information security risks
Cybersecurity	• Cyber attacks that breach our information network or failure to protect sensitive and confidential information of our stakeholders in accordance with applicable laws and contractual obligations may adversely impact our operations and client satisfaction or result in significant regulatory penalties. • **Impacted capitals:** Financial, Human, Intellectual and Manufactured	• Robust cybersecurity framework and controls • Multi-layered governance process with executive and Board oversight • Continued investment in technologies • Readiness to respond to incidents • Awareness programs and trainings • **Opportunity** – Cybersecurity services to the customer

Key / Emerging risks	Impact on Company	Mitigation / Opportunity
Data protection and privacy	• Failure to protect personal and sensitive information of our stakeholders in accordance with applicable laws may impact our operations or result in significant regulatory penalties. • **Impacted capitals:** Financial, Human and Intellectual	• Robust data privacy framework and controls • Privacy by design • Multi-layered governance process with executive and Board oversight • Preparedness for response to incidents • Awareness programs and trainings • Region-specific data protection controls and awareness campaigns
Cost inflation / Inability to improve margin	• If we are unable to run our operations effectively and with sustainable cost levers, our long-term profitability may be adversely affected. • **Impacted capitals:** Financial	• Effective operations with sustainable cost optimization levers • Automation and planned capex program focused on technology adoption
ESG	• If we are unable to demonstrate the outcome of our ESG program covering various areas such as climate change, GHG reductions, digital skilling, empowering local communities, diversity, responsible supply chains, compliance and governance, etc., our operations, reputation, access to capital and longer-term financial stability could be adversely impacted. • **Emerging risk aspect:** Expectations on ESG may change in future due to evolving stakeholders' expectations and disclosure requirements. • **Impacted capitals:** Financial, Human, Intellectual, Natural, Social & Relationship and Manufactured	• ESG 2030 goals and execution roadmap • Board level governance and oversight through dedicated ESG committee of the Board • **Opportunity** – Climate change related solutions and services to the customer.
Contractual liabilities	• Risk of clients demanding more favorable terms including onerous clauses related to the liability and our inability to adhere to contractual obligations with customers may lead to litigations, fines, and may adversely impact our reputation, revenue and profitability. • **Impacted capitals:** Social & Relationship and Financial	• Engaging clients on contractual terms through dedicated in-house team • Contract legal playbook with risk framework • Multi-layered governance process for contract approval • Dedicated teams to adhere, monitor and audit contractual obligations • Comprehensive Board level monitoring, reporting and governance
Complex and evolving regulatory environment	• If we are not able to comply with the existing complex regulatory landscape (e.g., immigration, wages, tax, sanctions), it could result in investigations, regulatory inquiries, litigation, fines, and negative client sentiments. • **Emerging risk aspect:** Evolving regulatory compliance, corporate governance and public disclosure requirements add uncertainty to our compliance policies. • **Impacted capitals:** Financial, Human, Intellectual, Social & Relationship and Natural	• Comprehensive compliance framework, controls and program • Awareness programs and trainings • Periodic compliance certification • Comprehensive monitoring, reporting and governance including Board oversight

APPENDIX


STRATEGY
Strategy and business objectives
Vision and mission
Values and culture
Strategic and stakeholder goals
Derived goals
PERFORMANCE EVALUATION AND RISK MANAGEMENT
Risk-enabled decision-making
Risk identification
Type of risks
Legal and compliance
Operational
Strategy execution
Level 1 Risk
Level 2 Risk
Level 3 Risk
Level 4 Risk
Level 5 Risk
Granularity
Sales
Delivery
Business enabling function
Impact groups
Risk assessment
Opportunity
Risk management
Treatment, mitigation and control implementation
Secondary and consequential risk assessment
Residual risk assessment and decision-making
Auditing, monitoring and reporting
Risk governance and disclosures
GOVERNANCE
8-layer governance
Board of Directors
Risk Management Committee (RMC) of the Board
Cybersecurity Sub-Committee
Risk councils
Office of risk management
Sub-risk councils
Unit risk councils
Project and account risk teams
Aligned lines of defense
iGRC platform
Intelligent risk analytics – Live Enterprise