



# FIGHTING FINANCIAL CRIME IN THE DIGITAL AGE

To state that financial crime is as old as capitalism wouldn't be far from the truth. But from the simplistic forgeries perpetrated by individuals, financial crime has rapidly progressed to significant corporate scandals and highly-skilled criminals using the latest technology to mastermind scandals. But on the other hand, there is a higher level of scrutiny in the market today as crime and compliance management has reached a level of maturity where regulators are able to better articulate expectations and compare established programs across financial institutions. Further, corporate and accounting scandals such as Enron and WorldCom have led to an increased expectation, both from companies' executive boards and shareholders, for concise and accurate reporting on compliance.

While the need for banks, insurers, and other financial service providers to abide by statutory requirements is a given, the effort and technology investment required to be made by these organizations to be compliant with regulations and combat financial crime is quite high, owing largely to the legacy monolithic applications they use. In a recent research report titled 'Compliance and Financial Crime Outlook 2018,' Greyhound Research, a leading global analyst firm, found that 73% organizations that are deemed compliant to statutory requirements are struggling with high costs and low operational efficiencies given the need to constantly integrate, maintain, and support a wide array of disconnected applications. This is worsened by the need to replace existing systems as part of the checklist to comply with revised statutory requirements.

## UPGRADING AGAINST FINANCIAL CRIME

The above research findings show the investment in and availability thereof of comprehensive technology platforms that allow financial institutions to leverage financial crime surveillance, detection, and event correlation along with regulatory reporting - all in a single platform. Oracle is one such technology provider, whose **Financial Crime and Compliance Management (FCCM) platform** is designed to **centrally manage and assess associated operational risks and controls** to improve and complement the organization's anti-money laundering (AML), fraud, KYC, and trading and broker compliance programs.

Infosys brings extensive experience in implementation and upgrades of a range of compliance products, including Oracle FCCM. Our AML solutions combine compliance expertise, frameworks, toolkits, clearly defined best practices, and comprehensive data-quality filters and partnerships with industry leaders such as Oracle FCCM, to offer **best-of-breed AML capabilities** and improve compliance programs.

A **banking and brokerage firm**, an Infosys client, wanted to replace their legacy platforms and move to a **comprehensive surveillance, case management, and regulatory reporting solution**. The client wanted to migrate from the obsolete Oracle Mantas to FCCM 8.0 to improve **compliance with the Bank Secrecy Act (BSA)/ Anti-Money Laundering program and Broker Compliance (BC)**. Being both a bank and broker, this migration was critical for the client from a compliance point of view.

Other objectives for the migration included upgrading the existing technology platform, bolster internal controls and surveillance, and simplify case management and regulatory reporting.

## ALERT-TO-CASE IN A MINUTE

Following software installation and environment set-up, we undertook data acquisition, data transformation according to FCCM specifications, and ingestion into the Oracle database. We ran multiple scenarios on the ingested data to find any indicative patterns, basis the set rules and patterns, of criminal activities like money laundering. FCCM has 12 scenarios, to which we developed and added 9 custom scenarios. These scenarios helped generate 'matches' scored for risk, which would be moved to the AML operations department as 'alerts' to be investigated and ultimately be promoted as 'cases' (in case money laundering activity was detected) and sent to the Enterprise Case Management (ECM) system.

The FCCM platform enabled **alert- to-case promotion** in a minute with the press of a button, with all supported information connected into it. The solution resulted in the client gaining an **integrated Enterprise Case Management system**. In addition, the Infosys team also deployed an **intranet-based web incident form** to raise AML alerts, and a **reference data utility** (used to deliver reference data management services to the banks) within FCCM. Leveraging industry standard tools and accelerators to improve the efficiency and performance of the team, Infosys team helped the client address findings of regulatory audits and fulfill regulatory requirements for BSA/ AML.



# FIGHTING FINANCIAL CRIME IN THE DIGITAL AGE : THE FIVE KEY TAKEAWAYS

- 1 **Strategize** to upgrade systems to ensure timely detection of financial crime and to keep pace with demands of compliance improvements by the regulator
- 2 **Build** custom scenarios based on the client's requirement to detect indicative patterns from ingested data
- 3 **Centralize** and integrate case management to allow for an enterprise-wide view of data to ensure consistency in reporting
- 4 **Establish** a comprehensive transparent audit trail to meet the changing regulatory needs and reduce reliance on IT teams for data and internal and regulatory reporting
- 5 **Provide** for market and reference data to support for rapid alert routing, better management of investigations, and hence escalation to the relevant teams

# BIG LEARNING:

The need to comply with stricter regulations and ensure protection against the increasingly sophisticated methods of financial crime is dictating that banks, insurance companies, trading, and brokerage firms hit the refresh button on their approach to combat financial crime. Infosys is witnessing this first hand and helping our clients build an appropriate line of defense. In our view, it is imperative for financial services firms to consolidate, centralize, and automate technology resources and related processes to ensure better use of data to improve the detection of suspicious actors and activities. Without such concerted efforts, firms are putting themselves at a higher risk of unwittingly becoming enablers of the next Enron, Cendant, or WorldCom.

## WE DID THIS FOR THEM. WE CAN DO IT FOR YOU.

To learn more about our financial crime and compliance solutions, reach out to us at [askus@infosys.com](mailto:askus@infosys.com)

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

**Infosys**<sup>®</sup>  
Navigate your next

© 2019 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.

Infosys.com | NYSE: INFY

Stay Connected     