

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

***63<sup>rd</sup> RBAP Annual National Convention  
and General Membership Meeting***

*Cebu City  
24 May 2016*



# Stark realities of Fraud

Fraud threats and attacks are becoming increasingly common and impact brand, competitive advantage, and shareholder value.

**Seniors lose \$36.48B each year to elder financial abuse**

## **FBI: \$1.2B Lost to Business Email Scams**

The FBI today warned about a significant spike in victims and dollar losses stemming from an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers. According to the FBI, *thieves stole nearly \$750 million in such scams from more than 7,000 victim companies in the U.S. between October 2013 and August 2015.*

**Citi May Face \$872M Charge over AIB Rouge Trader Suit**

## **Card fraud costs the US billions each year**

Payment card fraud cost the US \$7.9 billion last year alone, an increase of almost 60% from five years earlier.... In 2014, the US generated almost half of the world's total card fraud despite only comprising one-quarter of transactions. That's because the US had the least secure payment card ecosystem.

**J.P. Morgan Advisor Admits Stealing \$22M From Clients**

**City Odds Capital Director Charged in \$78 Million Pump and Dump Scheme**

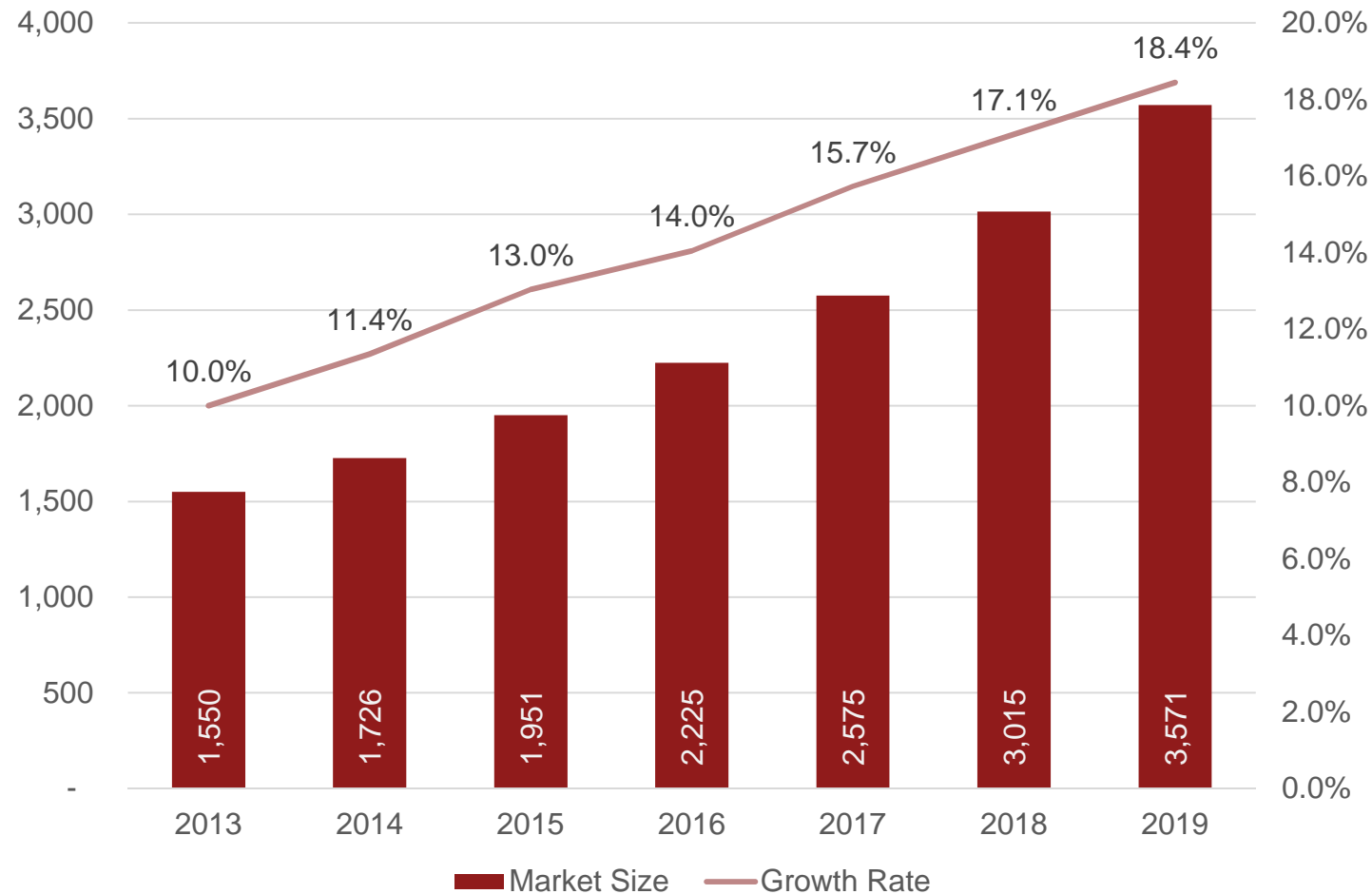
## **U.S. charges three in huge cyberfraud targeting JPMorgan, others**

U.S. prosecutors on Tuesday unveiled criminal charges accusing three men of running a sprawling array of hacking and fraud schemes, including a huge 2014 attack against JPMorgan Chase & Co, that generated hundreds of millions of dollars of illegal profit.

Prosecutors said the enterprise dated to 2007 and included pumping up stock prices, online casinos, payment processing for criminals, an illegal bitcoin exchange, and at least 75 shell companies and accounts around the world.

**FBI: Public & Private Sector Officials at Risk for Social Engineering to Gain Access to Victims' Data**

# Global fraud detection and prevention market revenue in banking & capital markets sector



**Expected to reach US\$3.6B billion by 2019, growing at an average CAGR of 15.6%, as compared to 5.6% for AML**

**This includes fraud authentication, analytics, reporting & visualization, and GRC**

Source: Markets and Markets; CAGR is 2014 to 2019; excludes insurance

# PwC's Financial Crimes Unit (FCU)

Financial crime is a major threat to the safety and soundness of financial institutions worldwide. As a result, it has become a top agenda item for The White House, Regulators, and both the Boards and CEOs of major financial institutions.

PwC's Financial Services Financial Crimes Unit (FCU) provides a holistic and integrated approach to navigating financial crimes. Four key areas collectively form the foundation for our financial crimes approach:

- 1) Cybersecurity, 2) Anti-Money Laundering and Sanctions (AML), 3) Fraud, and 4) Anti-Bribery and Corruption.

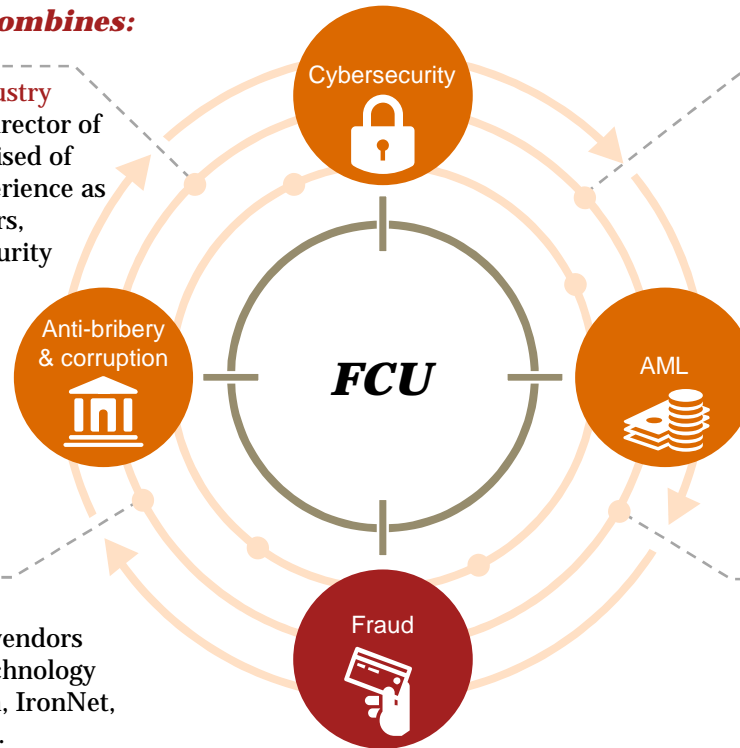
## ***Our team and our approach combines:***

**Deep subject matter expertise and industry experience**— Led by Former Deputy Director of the FBI, Sean Joyce, the FCU is comprised of more than 300 professionals with experience as former forensic investigators, regulators, law-enforcement officials, national security officials and seasoned consultants.

**Innovative and efficiency gaining tools**— We have a repository of tools and accelerators help our clients address their various financial crime challenges; including Game of Threats, Computer-Assisted Subject Examination and Investigations Tool (CASEit), our Sanctions investigations forensics toolkit and our fraud threat library and our fraud risk assessment apps.

**Strategic alliances with key vendors**— Our numerous relationships with key vendors enhance engagement efficiency and technology implementation; these include Tanium, IronNet, FireEye and Securonix (to name a few).

**Unparalleled knowledge of industry leading practices**—PwC has assisted many of the largest global, US and regional institutions across the banking & capital markets, asset management and insurance industries to fully address the complex business issue of financial crimes from board-level advice and strategy through execution.



# ***Fraud prevention building blocks***



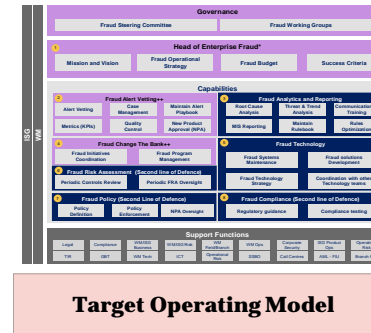
# Fraud Program and Operating Model

Assess the fraud program and operating model top-down, including performance metrics, design, and policy. Provide a vision for a target state operating model, and a roadmap to achieve, taking into account the institutions priorities.

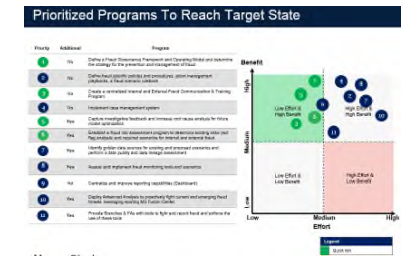
Approach	Deliverables	Samples
----------	--------------	---------

- ❑ Assess Key Performance Indicators (KPIs) for the anti-fraud program and operations
- ❑ Leverage Fraud Program Assessment Framework and benchmarks
- ❑ Evaluate the governance of enterprise-wide anti-fraud initiatives as well as day-to-day fraud management
- ❑ Create future state model defining the 1<sup>st</sup>, 2<sup>nd</sup>, and 3<sup>rd</sup> lines of defense
- ❑ Assess and improve policy including whistleblower hotlines, code of conduct, and anti-retaliation policies

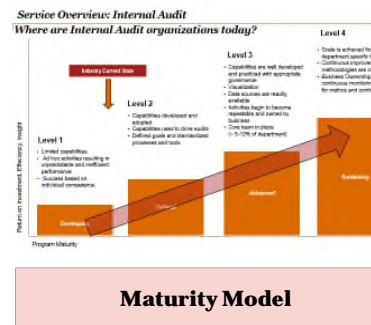
- Benchmarking & Peer Comparison
- Maturing Model
- Current State Observations (Key Themes) & Recommendations
- Magic Quadrant
- Prioritized Recommendations
- Target Operating Model
- Future State Org Chart and Staffing Model
- Implementation Roadmap



**Target Operating Model**



**Magic Quadrant Prioritized Recommendations**



**Maturity Model**

Area	Current State	Target State	Recommendations
1. Fraud Alert Settings	Level 1: Fragmented data, inconsistent data, no single source of truth, low visibility of fraud management activities.	Level 2: Data is integrated and available in a single source of truth, high visibility of fraud management activities.	1. Consolidate data from all systems into a single source of truth. 2. Implement a data governance framework. 3. Implement a data quality framework. 4. Implement a data security framework.
2. Fraud Analytics and Reporting	Level 1: Limited capabilities, no single source of truth, low visibility of fraud management activities.	Level 2: Capabilities developed and integrated, data sources are readily available, activities begin to leverage capabilities and expand the role.	1. Implement a data governance framework. 2. Implement a data quality framework. 3. Implement a data security framework. 4. Implement a data privacy framework.
3. Fraud Change The Bank	Level 1: Limited capabilities, no single source of truth, low visibility of fraud management activities.	Level 2: Capabilities developed and integrated, data sources are readily available, activities begin to leverage capabilities and expand the role.	1. Implement a data governance framework. 2. Implement a data quality framework. 3. Implement a data security framework. 4. Implement a data privacy framework.
4. Fraud Risk Assessment	Level 1: Limited capabilities, no single source of truth, low visibility of fraud management activities.	Level 2: Capabilities developed and integrated, data sources are readily available, activities begin to leverage capabilities and expand the role.	1. Implement a data governance framework. 2. Implement a data quality framework. 3. Implement a data security framework. 4. Implement a data privacy framework.
5. Fraud Policy	Level 1: Limited capabilities, no single source of truth, low visibility of fraud management activities.	Level 2: Capabilities developed and integrated, data sources are readily available, activities begin to leverage capabilities and expand the role.	1. Implement a data governance framework. 2. Implement a data quality framework. 3. Implement a data security framework. 4. Implement a data privacy framework.
6. Fraud Compliance	Level 1: Limited capabilities, no single source of truth, low visibility of fraud management activities.	Level 2: Capabilities developed and integrated, data sources are readily available, activities begin to leverage capabilities and expand the role.	1. Implement a data governance framework. 2. Implement a data quality framework. 3. Implement a data security framework. 4. Implement a data privacy framework.

**Peer Comparison**

# Fraud Risk

Informs our client of their inherent risks, provide a framework to quantify the impact of the control environment relative to those risks, and derive inherent risk, and possible areas for improvement and where to make future anti-fraud investments

Approach	Deliverables	Samples
----------	--------------	---------

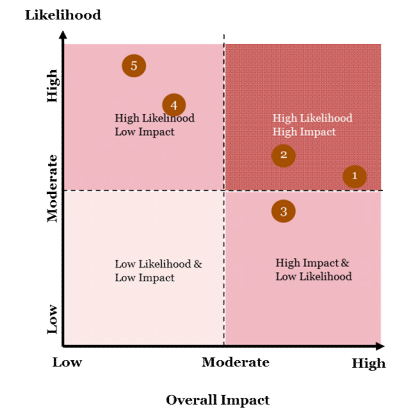
- ❑ Evaluate and prioritize fraud threats based on historic, known, and emerging fraud trends
- ❑ Estimate severity and likelihood of fraud risk events, and inventory existing mitigating factors
- ❑ Quantify the impact of existing controls in order to assess residual risks and recommend next steps
- ❑ Leverage PwC's Fraud Taxonomy and Threat Library and other accelerators

- Fraud Risk Assessment (FRA) Methodology
- Fraud Threats Library
- Risk Scoring Model
- FRA Questionnaires
- FRA Control Library
- FRA Heat Maps of Risks
- Residual Risk Prioritization
- FRA Final Report & Recommendations

Financial Loss	Negligible financial loss	Insignificant financial loss	Immaterial financial loss	Significant financial loss	Material financial loss
Reputational Risk	Remote chance of adverse publicity or reputational damage	Low probability of adverse publicity or reputational damage	Moderate probability of adverse publicity or reputational damage	High probability of adverse publicity or reputational damage	Very high probability of adverse publicity or reputational damage
Regulatory Risk	Remote chance of future compliance fines or penalties, no increase in regulatory focus	Inconsequential or minor compliance penalties, minimal increase in regulatory focus	Moderate compliance penalties, moderate increase in regulatory focus	Significant compliance penalties, significant increase in regulatory focus	Severe compliance penalties, customer restriction, or class action suits, severe increase in regulatory focus

		Impact				
		1	2	3	4	5
Likelihood	1 Low	1	1.75	2.5	3.25	4
	2 Moderate-Low	1.25	2	2.75	3.5	4.25
	3 Moderate	1.5	2.25	3	3.75	4.5
	4 High	1.75	2.5	3.25	4	4.75
	5 Very High	2	2.75	3.5	4.25	5

**Risk Scoring Model**



**Residual Risk Prioritization**



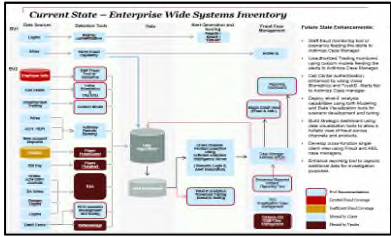
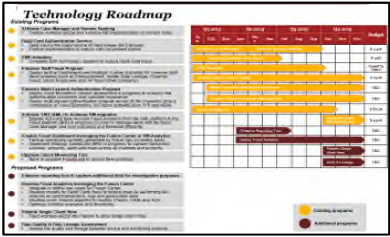
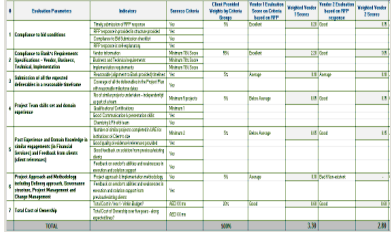

# Fraud Controls Design and Effectiveness

Detailed assessment and evaluation of anti-fraud processes and controls relative to identified risks in order to identify weaknesses and areas for improvement; provides a forward looking strategy for improving controls.

Approach	Deliverables	Samples
<ul style="list-style-type: none"> <li>❑ Evaluate the design of existing controls and procedures; including end-to-end process flows</li> <li>❑ Assess procedures relative to anti-fraud policies</li> <li>❑ Apply analytics to assess the effectiveness of controls and to identify opportunities for improvement</li> <li>❑ Perform “penetration testing” to further assess the efficiency and effectiveness of current controls</li> <li>❑ Provide tactical (e.g., new rules or processes) and strategic recommendations</li> </ul>	<ul style="list-style-type: none"> <li>➤ Business Process Flows (for fraud processes and controls)</li> <li>➤ Fraud Controls Testing Plan</li> <li>➤ Fraud Control Effectiveness Assessment</li> <li>➤ Fraud Control Evaluation</li> <li>➤ Assessment Dashboard</li> <li>➤ Tactical and Strategic Recommendations</li> </ul>	<div style="display: flex; justify-content: space-around;"> <div data-bbox="1513 494 1893 751"> <p><b>Business Process flows, fraud risk and controls</b></p> </div> <div data-bbox="1982 508 2361 836"> <p><b>Threats Library</b></p> </div> </div> <div style="display: flex; justify-content: space-around; margin-top: 20px;"> <div data-bbox="1544 922 1923 1179"> <p><b>Controls Evaluation</b></p> </div> <div data-bbox="1989 908 2369 1179"> <p><b>Fraud Control Effectiveness Assessment Dashboard</b></p> </div> </div>

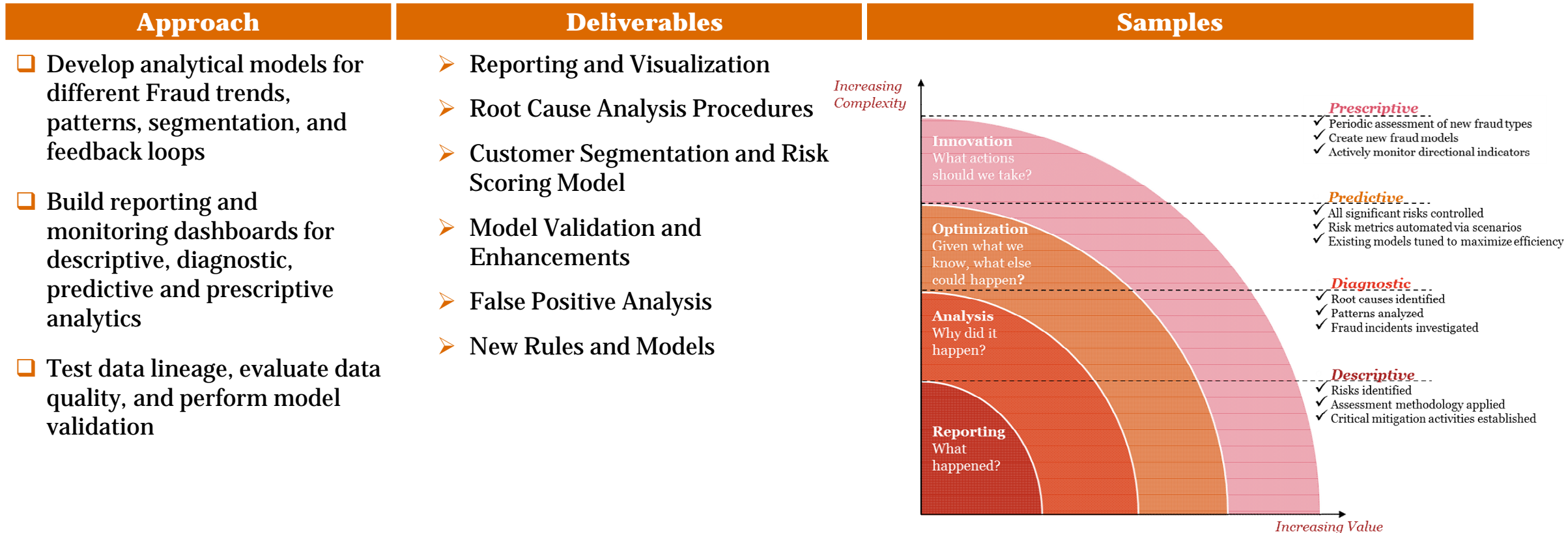
# Fraud Technology

Enable clients to inventory existing tools and their effectiveness; inform clients of the specific tactical and infrastructure needs for implementing new technologies; empower clients to effectively evaluate new solutions; help clients implement technologies and controls.

Approach	Deliverables	Samples
<ul style="list-style-type: none"> <li>❑ Perform Current State Assessment</li> </ul>	<ul style="list-style-type: none"> <li>➤ Current State Technology Inventory</li> </ul>	 <p data-bbox="1528 735 1905 763"><b>Current State Systems Inventory</b></p>
<ul style="list-style-type: none"> <li>❑ Gather Business Requirements</li> </ul>	<ul style="list-style-type: none"> <li>➤ Technology Roadmap</li> </ul>	 <p data-bbox="1979 735 2356 763"><b>Technology Roadmap</b></p>
<ul style="list-style-type: none"> <li>❑ Perform Vendor Selection</li> </ul>	<ul style="list-style-type: none"> <li>➤ Vendor Selection Scorecard</li> </ul>	 <p data-bbox="1528 1106 1905 1135"><b>Vendor Selection Scorecard</b></p>
<ul style="list-style-type: none"> <li>❑ Implement Relevant Technology Solution</li> </ul>	<ul style="list-style-type: none"> <li>➤ Business Requirements Document (for any new implementations)</li> </ul>	 <p data-bbox="1979 1178 2356 1230"><b>Business and Functional Requirements Documents</b></p>
<ul style="list-style-type: none"> <li>❑ Post Implementation Testing</li> </ul>	<ul style="list-style-type: none"> <li>➤ Functional Requirements Document</li> </ul>	
<ul style="list-style-type: none"> <li>❑ Collaborate with Vendors (for JBR firms)</li> </ul>	<ul style="list-style-type: none"> <li>➤ Test Plan and Test Scenarios</li> </ul>	

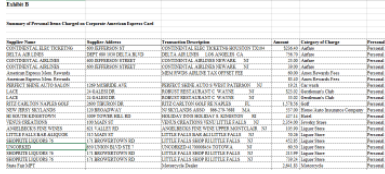
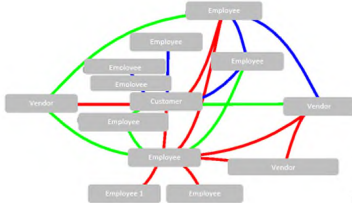
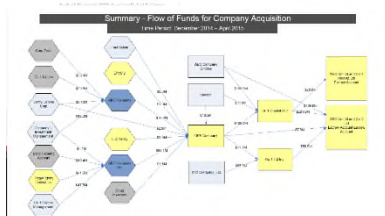
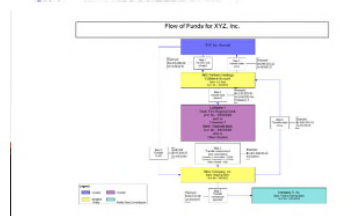
# Fraud Analytics

Help clients implement improved Fraud Analytics functions to more effectively monitor and improve their programs on an ongoing basis, including reporting, root cause analysis, control testing and optimization, and innovation.



# Fraud Investigations and Readiness

Provide on-call forensic investigation response to high profile fraud and other risk events; help institutions assess and improve their internal fraud investigative function.

Approach	Deliverables	Samples
<ul style="list-style-type: none"> <li>❑ Conduct reactive fraud investigations and root cause analyses</li> <li>❑ Create incident readiness and response plans, including tactical remediation and crisis management</li> <li>❑ Help institutions assess and improve their internal investigative capabilities, including desktop procedures, case management, technology, analytics, and data management</li> <li>❑ Improve Fraud awareness, including training, tone-at-the-top and regulatory compliance</li> </ul>	<ul style="list-style-type: none"> <li>➤ Forensic Reporting &amp; Findings of high profile events</li> <li>➤ Fraud Response Playbook</li> <li>➤ On-Call Forensic Retainer</li> <li>➤ Operating model, and roadmap for improved fraud investigative function.</li> </ul>	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;">  <p><b>Expense Analysis</b></p> </div> <div style="width: 50%;">  <p><b>Link Analysis</b></p> </div> <div style="width: 50%;">  <p><b>Entities Analysis</b></p> </div> <div style="width: 50%;">  <p><b>Flow of Funds Analysis</b></p> </div> </div>

# Sample control points – customer deposit account fraud

External Threat Management	Account Opening	Deposit	Authentication	Activity	Payment	Case Management	Analytics
App store / dark web monitoring	Identity verification	Funding source verification	Biometric, out of band, knowledge based	Non financial behavioral, endpoint malware detection	Transaction monitoring	Fraud event tracking and record keeping	Control enhancements
<ul style="list-style-type: none"> <li>• Spoofed website monitoring</li> <li>• App Store Monitoring</li> <li>• Monitoring of “dark web” sites for Discover customer credentials</li> <li>• Customer and employee education</li> <li>• Social media monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• CIP and proof of identity</li> <li>• Authentication e.g., “out-of-wallet” questions</li> <li>• Data sharing/ consortium based screening</li> <li>• Analytics and customer/ acct risk scoring</li> </ul>	<ul style="list-style-type: none"> <li>• Online sign-in to counterparty bank</li> <li>• Micro-deposit from originating account</li> <li>• Consortium based screening</li> <li>• Enhanced deposit hold policy</li> </ul>	<ul style="list-style-type: none"> <li>• Adaptive authentication</li> <li>• Out of band</li> <li>• Voice, fingerprint, and iris recognition</li> <li>• User gesture recognition</li> <li>• Hard/ soft token</li> <li>• Security questions</li> <li>• Call center/ IVR analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Trusted device identification</li> <li>• Geo location based pre-authentication</li> <li>• Clickstream analysis</li> <li>• Payee name verification (PNV)</li> </ul>	<ul style="list-style-type: none"> <li>• Positive pay</li> <li>• 4 eye review</li> <li>• Rules-based transaction monitoring</li> <li>• Predictive modeling</li> <li>• Alert/ case management</li> </ul>	<ul style="list-style-type: none"> <li>• Identification and maintenance of Fraud cases and related KRIs, KPIs</li> <li>• Maintain list of reviewed/ existed customers</li> <li>• Controls to prevent re-entry of exited customers</li> </ul>	<ul style="list-style-type: none"> <li>• Statistical analysis of Fraud event KPIs to derive new or enhance existing controls</li> </ul>
<ul style="list-style-type: none"> <li>• Cyveillance</li> <li>• Kaspersky Lab</li> <li>• myNetWatchman</li> <li>• Phishlabs</li> </ul>	<ul style="list-style-type: none"> <li>• Andera</li> <li>• ChexSystems</li> <li>• Early Warning</li> <li>• Equifax</li> <li>• EFiserv</li> <li>• CashEdge</li> <li>• Idology</li> <li>• Experian</li> <li>• LexisNexis</li> <li>• Teletrack</li> <li>• TransUnion</li> </ul>	<ul style="list-style-type: none"> <li>• Andera</li> <li>• CashEdge,</li> <li>• Forte Payment Systems</li> </ul>	<ul style="list-style-type: none"> <li>• RSA Adaptive</li> <li>• Agnitio Voice ID</li> <li>• BioCatch</li> <li>• Nuance</li> <li>• Pindrop Security</li> <li>• Equifax</li> <li>• Experian</li> <li>• LexisNexis</li> <li>• TransUnion</li> </ul>	<ul style="list-style-type: none"> <li>• CheckFree</li> <li>• Crealogix</li> <li>• Entrust</li> <li>• IBM Trusteer</li> <li>• Iovation</li> <li>• iDetect</li> <li>• Kaspersky Lab</li> <li>• ThreatMetrix</li> <li>• TrustDefender</li> <li>• Silver Bullet’s Ranger</li> </ul>	<ul style="list-style-type: none"> <li>• Actimize</li> <li>• iDetect</li> <li>• Intellinx</li> <li>• FICO Falcon</li> <li>• BAE Systems</li> <li>• RSA Adaptive</li> <li>• SAS</li> <li>• Memento</li> <li>• Guardian Analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Actimize Enterprise Case Manager</li> <li>• BAE Systems</li> <li>• IBM BPM</li> <li>• iDetect</li> <li>• Intellinx</li> <li>• SAS</li> </ul>	<ul style="list-style-type: none"> <li>• IBM (SPSS)</li> <li>• SAP</li> <li>• SAS</li> <li>• Teradata</li> <li>• Theta-ray</li> </ul>

# Speaker's profile

*Sam Samod*  
*Director*

*Tel: +66 6-1417-4424*

*Email: samod.sam@th.pwc.com*



## Qualifications and memberships:

- University of Minnesota, Minneapolis
  - MBA in Management Information Systems and Finance
  - BS in Management Information Systems
- Project Management Professional (PMP), Project Management Institute
- Certified Management Consultant (CMC), Canadian Association of Management Consultants

## Professional background:

- Sam, a secondee from PwC New York, brings eighteen years of experience in data analytics, anti-money laundering, anti-fraud, regulatory compliance, customer relationship management (CRM), consumer lending, collections, and risk management. His background includes broad range of financial information systems and applications covering retail banking, wealth management and capital markets in North America, Europe, and Asia.

## Relevant experience:

- Developed a reference architecture to consolidate and aggregate enterprise data at one of the top banks in Canada. Leveraged Oracle Financial Services Analytical Applications (OFSAA) Framework for data aggregation and reporting to ensure compliance with BCBS 239.
- Managed a Fraud Analytics workstream at a large global wealth management institution. Developed a fraud taxonomy and use cases for the proof-of-concept and the strategic roadmap. Demonstrated benefits of analytics to introduce additional controls and optimize existing detection rules. Identified data requirements to support use cases specific products and channels.
- Conducted Customer Risk Rating model calibration at a leading commercial bank. Reviewed algorithms and risk dimensions of GlobalVision's Patriot Officer. Developed an approach to calibration the model and adjusted one of the risk dimensions to reduce false positives. Realized 20% reduction in the total high risk population and 82% reduction in the number of alerts.
- Led an algorithm development team on an AML Look Back project at one of the Fortune 500 financial services firms. Assessed transaction monitoring requirements and mapped them back to key data elements. Identified key risks, performed statistical analysis, generated alerts, and recalibrated final algorithms based on investigations feedback. Aligned processes with IT solutions including Aster, SAS, and Actimize.
- Led Data Analytics workstream in a multi-phase engagement to enhance AML transaction monitoring for Capital Markets with initial focus on wires and trade finance transactions. Conducted data mapping and assess data quality according to Oracle Mantas data ingestion requirements to drive alert generation, scenarios tuning, workflows, and user interfaces. Developed SAS Analytics environment to generate alerts based on custom scenarios.
- Managed high priority multi-workstream projects to centralize AML technology and business processes of all a global bank's Private Banking, Wealth Management, and Capital Markets business units globally.

---

# ***Thank you!***

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.