AGENDA

I. Defining the Universe of Prepaid Cards
   • Prepaid Cards & Key Participants Defined
   • Primary sources of Funding & Reloading
   • Card Issuance, Usage, Limitations & Demand
   • AML Risk Factors

II. What is the Regulatory Focus on Prepaid Cards?
   • Evolution of regulatory considerations
   • Current regulatory perception
   • Unaddressed inherent risks

III. Prepaid Card Monitoring
   • Existing Software and infrastructure Challenges
   • Traditional Monitoring Software Shortcomings
   • The Future of Prepaid Card monitoring

IV. Lesson Learned

V. Questions

VI. Sources Cited & Additional Reference

VII. Biographies
DEFINING THE UNIVERSE OF PREPAID CARDS
There are multiple users and issuers of prepaid cards… and the list is growing.
PREPAID CARDS DEFINED

There are two main categories of prepaid cards.

**Prepaid Cards**

- A prepaid card functions like credit and debit cards but is not linked to a bank account. Typically has no value until it is “loaded.”

**Types of Prepaid Cards**

- Closed Loop prepaid cards are merchant specific. The card can only be used at the specific merchant. For instance, a JC Penney card can only be used at JC Penney. Closed system cards are typically non-reloadable but can offer a reload feature.

- Open Loop prepaid cards are usually associated with a specific electronic payment network such as Visa or Mastercard. They can be used at any businesses accepting cards within those networks. Open loop cards are referred to as General Purpose Reloadable (GPR) prepaid cards. They have grown in popularity as an alternative to traditional checking accounts.
Prepaid cards follow the traditional bank or debit card processing environment…

Issuer
- A bank that offers card association branded payment cards directly to consumers.
- Issues payment to the merchant acquirer on behalf of its customer

Issuer Processor
- A financial institution that issues the card to the bank customer.

Networks
- Dictate where the cards can be used
- Facilitate the payment process between card users, merchant and the card issuer
- Examples are Visa Mastercard and ATM networks

Merchant Processor
- Responsible for the settlement of electronic payment transactions for merchants

Merchant Acquirer
- Bank or financial institution that processes credit and or debit card payments for products or services for a merchant

Merchant
- Point of sale or payment

…however, GPR has three additional participants not included in the traditional bank debit card environment

- **Program Manager**
  - Under contract with a financial institution
  - Designs and runs the card program
  - Supports issuance, delivery and distribution of GPR Cards
  - Sometimes responsible for providing customer service

- **Distributor/Seller**
  - Represents Multiple GPR prepaid card products
  - Develops a contract network of sellers by shipping inventories to locations
  - Sellers ranging from big box retailers, regional grocers, drug store chains, internet retailers, bodegas

- **Load/Reload Sites & Networks**
  - Retail merchant or MSB operating a network to provide reloadable services
  - B&M and virtual reload sites
  - Bank branch locations (i.e., Chase, US Bank, PNC and Regions Banks)
There are multiple sources of funding for loading/reloading prepaid cards

- Cash
- Direct deposit
- ACH transfers from DDAs
- Electronic Transfers from debit and credit cards
- Transfers between prepaid debit cards
- PayPal
Who are the typical purchasers of Prepaid Cards

- **Unbanked consumers** – these are consumers that have no bank account for a number of reasons such as service charges, etc. Prepaid cards are used to manage spending, for online purchases and some cards can be utilized for ATM currency withdrawals.

- **Underbanked** – these consumers typically use nonbank financial service providers to conduct routine transactions such as check cashing and/or bill pay. Occasionally use as a credit card substitute.

- **Fully Banked** – prepaid debit cards are utilized as “companion” products to their traditional bank products. They are used for vacations, children away at school, cash management, etc.
Limitations on prepaid cards can be valuable tools for deterring money laundering.

**Usage**
- Brick and mortar retail purchases at participating merchants
- online purchases,
- bill pay
- ATM cash withdrawals.

**Limitations**
- Card Value Limits
- Value Load Limits
- spending and Cash withdrawal limits
- Geographical limits
- Issuance limits per person, account, etc.

**Other limitations**
- Activation fees
- Monthly service charges
- Transaction fees
- Inactivity fees
According to the Center for Financial Services Innovation, in 2012 prepaid cards were used in
– 1.3 billion transactions
– totaling $77 billion.

The amount loaded onto prepaid cards is expected to increase 42% by the end of 2014 according to the Consumer Financial Protection Bureau.

Source: ABC News, Worst and Best Prepaid Debit Cards Rated, Susanna Kim, July 31, 2013
Projected Growth Estimates on the demand for Prepaid debit and Payroll cards
WHAT IS THE RISK
Various attributes making prepaid cards attractive to money launderers

- Anonymity
- Transferability
- Transportability
- Easy to purchase
- Accessibility
- Immediate liquidity
# AML RISK FACTORS

## Areas of Money Laundering Opportunities

<table>
<thead>
<tr>
<th>Low Risk</th>
<th>Medium Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed Load Amount by load transaction</td>
<td>Some Limits</td>
<td>Unlimited Load Amount by load transaction</td>
</tr>
<tr>
<td>Limit on Total Load Amount</td>
<td>Some Limits</td>
<td>Unlimited on Total Load Amount</td>
</tr>
<tr>
<td>One-time Load</td>
<td></td>
<td>Reloadable</td>
</tr>
<tr>
<td>Purchaser is an Existing Customer of Issuing Bank</td>
<td></td>
<td>Purchased Has No Account Relationship to Issuing Bank</td>
</tr>
<tr>
<td>Full Identification &amp; Verification of Purchaser</td>
<td></td>
<td>No Identification &amp; Verification of Purchaser</td>
</tr>
<tr>
<td>Known Card Holder</td>
<td></td>
<td>Anonymous Card Holder</td>
</tr>
<tr>
<td>Source of Funds DDA of Purchaser at Issuing Bank</td>
<td>Source of Funds Credit Card</td>
<td>Source of Funds Cash, Other Prepaid Cards</td>
</tr>
<tr>
<td>Source of Funds Domestic Load, Domestic Use</td>
<td>Domestic Load, Domestic Use</td>
<td>International Load, International Use</td>
</tr>
</tbody>
</table>

Source: Bryan Cave & Prepaid Cards: Vulnerable to Money Laundering Feb. 2007
AML RISK FACTORS

Areas of Money Laundering Opportunities

- International Debit Cards can withdraw money anywhere in the world and the customer is not required to have an account with the issuing financial institution
  - High risk geographic locations
  - Countries subject to OFAC sanctions and those already identified by the financial institution based on prior experience
  - Countries identified as supporting international terrorism

- Monitoring applications lacking internal controls – both automated and manual
  - Infrequent independent testing
  - Inadequate training

- Know your customer (KYC)
  - Customers or 3rd parties located in HIDTA and HIFCA
  - Foreign financial institutions both banks and foreign MSBs
  - Non-bank financial institutions (i.e., casinos and card clubs, dealers in precious metals, stones, etc.)

- Third Party Agents
  - Financial Institutions contracting with 3rd party agents accept the risk related to the services provided
  - Appropriate due diligence review is absolutely necessary

- Issuers
  - Cards issued to non-customers
  - False/stolen identification used for the purchase of prepaid cards
AML RISK FACTORS

Risk mitigation can reduce money laundering exposure

- Identification and verification measures
- Employee Training
- Transaction Monitoring
- Value Limits
  - Funding
  - Reloading
- Funding Methods
WHAT IS THE REGULATORY FOCUS?
### EVOLUTION OF REGULATORY FOCUS

<table>
<thead>
<tr>
<th>Statutes/Regulation</th>
<th>Relevant Provisions/Guidance</th>
</tr>
</thead>
</table>
• Treasury requires banks to keep records to identify, report laundering operations  
• Must report all single transactions above $10,000 and multiple transactions totaling more than $10,000 to or from a single account in one day (CTRs)  
• Require sellers of prepaid access cards to:  
  o Develop and implement an effective AML program;  
  o Report suspicious activity; and  
  o Comply with recordkeeping requirements related to customer identifying information and transactional data. |
| **USA PATRIOT Act (2001)** | • Requires mandatory I.D. checks for U.S. bank patrons  
• AML extended to Financial Services industry (Programs & SARs required for some)  
• Resources to track transactions in underground/alternative banking systems |
| **Treasury Regs (FinCEN and OFAC)** | • FinCEN issued a final rule on prepaid access under the BSA that imposed BSA/AML regulatory obligations for both “providers” and “sellers” of prepaid access cards on July 27, 2011. Providers are usually the program manager or the issuing financial institution. |
| **Bank Secrecy Act Anti-Money Laundering Examination Manual** | • FFIEC BSA/AML Examination Manual  
• FFIEC Guidance on E-Cash:  
| **Industry Self Regulation** | • NBPCA Issued AML Guidance  
• Card Networks Guidance |
| **Other statutes** | • 1986 Money Laundering Control Act (criminalized money laundering)  
• 1988 Money Laundering Prosecution Improvement Act (expanded coverage of crimes)  
• 1992 Annunzio-Wylie Money Laundering Suppression Act (added SARs to FDI Act)  
• 1994 Money Laundering Suppression Act (made CTRs easier to file)  
• 1998 Money Laundering & Financial Crimes Strategy Act (bank examiners learn AML) |
PREPAID CARD MONITORING
The complexity is not in monitoring, but rather data volumes, lack of available information and the consistency of data sources.
Payment Processors experience daily high volumes, low dollar amounts requiring ongoing Data Control Log Reviews to ensure controls are reliable.
THE PARADIGM SHIFT

Pitfalls when trying to apply Traditional Banking product monitoring concepts to Prepaid Cards

- Limited availability of Customer Information
  Many existing transaction monitoring and customer risk rating systems have required fields that cannot be left unpopulated
  - Direct KYC will not be easy to obtain unless the card holder is also a Bank Customer
  - You are reliant upon the data capture standards of your Program Managers, Distributors, Sellers, and Agents
  - In some instances, PPC may not require CIP (e.g. low dollar gift cards)

- Higher Volume of Transaction Data (#’s)
  Many existing transaction monitoring environments do not scale up well
  - Since PPC’s are a cross between a traditional checking/savings accounts, debit cards, and credit cards- the volume of activity is significantly higher for a given card holder than a traditional bank account holder

- Lower Transactions Values ($’s)
  Existing monitoring scenarios have thresholds applicable only to higher dollar events
  - Load limits, usage limits, withdrawal limits, balance limits all contribute to lower transactional values
  - As PPCs continue to expand into the unbanked and underbanked community, average transaction values may be significantly lower than traditional checking and savings account activity

- Limited to a Card Holder level view of PPC owners
  There may not be any obvious links between card holders, making it increasingly difficult to obtain a Customer level view of activity for monitoring
A Sample PPC Usage Risk Matrix

<table>
<thead>
<tr>
<th>PPC Transaction Types ↓</th>
<th>Attributes of PPC Transactions over Time →</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Volume</td>
</tr>
<tr>
<td>Load (Inbound)</td>
<td>High, Moderate, Low</td>
</tr>
<tr>
<td>Reload (Inbound)</td>
<td>...</td>
</tr>
<tr>
<td>Transfer (Inbound)</td>
<td>...</td>
</tr>
<tr>
<td>Transfer (Outbound)</td>
<td>...</td>
</tr>
<tr>
<td>Merchant Purchase (Outbound)</td>
<td>...</td>
</tr>
<tr>
<td>ATM Withdrawal (Outbound)</td>
<td>...</td>
</tr>
<tr>
<td>Bill Payment (Outbound)</td>
<td>...</td>
</tr>
<tr>
<td>[User defined transaction type]</td>
<td>...</td>
</tr>
</tbody>
</table>

- Transaction Types (rows above) represent groupings of similar types of Customer activity that PPC are involved in
- Attributes (columns across) represent dimensions that are measurable
- Each intersection point in the matrix represents a potential consideration that can be used to design
  - Customer Risk Rating scoring components
  - Transaction Monitoring scenarios
Some of today’s monitoring rules for PPCs are typically existing scenarios for cash and wires, retrofitted to PPC

### Scenario/Rules

<table>
<thead>
<tr>
<th>Scenario/Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excessive Daily Outgoing Fund Transfers</td>
<td>Covers transfers from Card to Card and from Card to Account; Monitors for Layering scenarios</td>
</tr>
<tr>
<td>Excessive Daily Incoming High Risk Fund Transfers</td>
<td>Covers transfers from Card to Card and from Card to Account; Monitors for Layering scenarios</td>
</tr>
<tr>
<td>Excessive Daily Outgoing High Risk Fund Transfers</td>
<td>Covers transfers from Card to Card and from Card to Account; Monitors for Layering scenarios</td>
</tr>
<tr>
<td>Filter Accounts On Accounts White List</td>
<td>Processor level accounts are being excluded</td>
</tr>
<tr>
<td>Flow Through of Funds (Long Period)</td>
<td>Covers Cash Deposit/ Cash Withdrawal scenario over a rolling week look back</td>
</tr>
<tr>
<td>Cash deposit and cash withdrawal on the same day</td>
<td>Covers &quot;Cash deposit and cash withdrawal on the same day&quot; typology</td>
</tr>
<tr>
<td>Increase in ATM withdrawals Value Following Changes to Client Data</td>
<td>Covers unusual ATM activity following a Customer information adjustment</td>
</tr>
<tr>
<td>Increase in Cash Equivalent Deposits Value Following Changes to Client Data</td>
<td>Covers unusual Cash/Cash Equivalent deposits following a Customer information adjustment</td>
</tr>
<tr>
<td>Increase in Cash Equivalent Withdrawals Value Following Changes to Client Data</td>
<td>Covers unusual Cash/Cash Equivalent withdrawals following a Customer information adjustment</td>
</tr>
</tbody>
</table>

Consider developing scenarios that look beyond the Card holder level
- Address/House-holding level: concentration of card holders in a confined geographic location
- Merchant level: merchants with abnormally high volumes may require periodic EDD reviews
- Processor level: relationships with processors may need to revisited frequently
- Phone level: concentration of card holders utilizing similar demographic information such as Phone
- Agent level (if possible): agents of distributors, program managers, or sellers warrant some level of scrutiny
Some of today’s customer risk rating rules for PPC holders are the same for any banking product.

<table>
<thead>
<tr>
<th>Risk Ranking Factors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAICS Code</td>
<td>Covers scoring of specific industry classifications</td>
</tr>
<tr>
<td>TIN Type</td>
<td>Covers type of Governmental ID</td>
</tr>
<tr>
<td>KYC Question responses</td>
<td>Customer onboarding questions</td>
</tr>
<tr>
<td>Zip Code in HIDTA, HIFCA</td>
<td>Customer/Account address in high risk area</td>
</tr>
<tr>
<td>Initial Source of Funds</td>
<td>Covers bank accounts funded with large denominations</td>
</tr>
<tr>
<td>Client Net Worth</td>
<td>Covers affluent clientele</td>
</tr>
<tr>
<td>Account Age</td>
<td>Covers relative length of relationship</td>
</tr>
<tr>
<td>SAR history</td>
<td>Covers Customers with a history of Suspicious Activity</td>
</tr>
<tr>
<td>Occupation</td>
<td>Covers Customers in High Risk positions</td>
</tr>
<tr>
<td>Account Opening Channel</td>
<td>Covers Face-to-Face and Non Face-to-Face relationships</td>
</tr>
</tbody>
</table>

Consider developing risk factors that takes non-traditional information into consideration:
- Ongoing funding sources (for reloadable cards)
- Using locations of card load, reload, and usage sites to measure the geographic “coverage area” of a PPC customer
- Measuring deviations from expected activity for a given card type
LESSONS LEARNED

What we’ve seen from working with Bank’s & Processors

The demand for prepaid cards will continue to grow to fulfil consumer needs. The anonymity, transferability and transportability of prepaid cards make it attractive to persons committing money laundering, therefore requiring closer surveillance through tighter controls.

Distributors of prepaid cards need to ensure that their internal controls for purchasing and reloading adequately address the associated risks.

Prepaid Card Program Considerations

– Potential for additional card limitations (# cards per holder, loads, reload, usage, or balance levels) to be revisited if BSA/AML monitoring is not tailored towards/does not address PPC product risks.

Regulatory Considerations

– Ease of transfer and anonymity of certain PPC products are inherent risks despite current regulations.

– More practical guidance is needed on how to monitor PPC products given the clear differences from traditional banking products.

Technology Considerations

– Current software packages support traditional banking products associated to an account holder.
LESSONS LEARNED

What we’ve seen from working with Bank’s & Processors

- Technology Considerations - continued
  - Ad-hoc Data analytics may be necessary to circumvent limitation in your current Transaction Monitoring and Customer Risk Rating systems
  - If the identities of card holders cannot be determined, it may make sense to rely on 3rd party information sources to truly Know-Your-Customers
  - If possible, demand that Program Managers, Processors, Distributors adhere to a set of data capture standards that you enforce; this will reduce mapping needs when the data reaches your organization
Pew Foundation Research Study (2012)
Loaded with Uncertainty: Are Prepaid Cards a Smart Alternative to Checking Accounts? (Pew Charitable Trusts)
(http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Prepaid_Cards/Pew_prepaid_checking_report.pdf)

Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs (NBPCA)
(http://www.nbpca.com/docs/nbpca-aml-recommended-practices-080220.pdf)

Wolfsberg Guidance on Prepaid & Stored Value Cards (2011)
Wolfsberg Guidance on Prepaid and Stored Value Cards (The Wolfsberg Group)

Have Anti-Money Laundering Measures Kept Pace with the Rapid Growth of GPR Prepaid Cards? (Douglas King)
(https://www.frbatlanta.org/documents/rprf/rprf_pubs/130117_wp.pdf)

Consumer’ Use of Prepaid Cards (2012)
A Transaction-Based Analysis (Stephanie M. Wilshusen, Robert M. Hunt, James van Opstal, FRB Philadelphia & Rachel Schneider, Center for Financial Services Innovation)

Prepaid Cards (2007)
Vulnerable to Money Laundering? (Stanley Sienkiewicz, FRB Philadelphia)

ABC World News (2013)
Worst and Best Prepaid Debit Cards Rated (Susanna Kim)
Sources Cited and Additional Reference

Listing of Cited Sources and Additional Reference Sources

- Aite Group
  The Contenders: Prepaid Debit and Payroll Cards Reach Ubiquity (2013)

- FATF
  Money Laundering Using New Payment Methods October 2010
Craig D. Stone is a Senior Director with Alvarez & Marsal Financial Industry Regulatory Advisory Services in Houston, Texas. Mr. Stone brings a unique and varied background with substantial and proven financial service experience, focusing on risk identification and controls. With more than 27 years in regulatory bank supervision, Mr. Stone has been directly involved in troubled bank oversight, compliance risk management and fiduciary activities risks assessment. Mr. Stone possess a broad set of skills with experience in wide-variety of banking activities including enterprise-wide risk management, corporate governance and consumer compliance.

Prior to joining A&M, Mr. Stone was the Deputy Ombudsman for the Comptroller of the Currency (OCC) charged with the day-to-day management of the Customer Assistance Group (CAG). In this role, he was responsible for leading a staff of more than 70 professionals including, National Bank Examiners, consumer compliance specialists and information technology experts. Mr. Stone was a key contributor in the creation of early warning tools and measures to identify emerging industry and/or institution specific risks, through the leveraging of customer complaints received by CAG. In addition, Mr. Stone led or provided support in the analysis and processing of complex regulatory disputes and appeals received by the Ombudsman from national banks. Furthermore, he pioneered the concept and branding of a consumer-based internet site which automated select business support functions and expanded customer self-service.

Previously, Mr. Stone served as a National Bank Examiner with a focus on retail banking and compliance management. In this role, he was directly involved in reviews and examinations of many of the largest banking organizations in the country. Mr. Stone has also provided expert witness testimony in Federal Court on allegations involving fraudulent lending and improper insider transactions. Mr. Stone began his regulatory career in the analysis and examination of bank fiduciary activities and asset management, earning a National Trust Examiner commission.

Mr. Stone received a bachelor’s degree in Banking and Finance from Texas State University. He later attended the United States Treasury Executive Leadership Program at Charlottesville, Virginia. Mr. Stone is a founding member of the International Network of Financial Service Ombudsman. In addition, he is a frequent speaker at industry conferences on Financial Institution Risks, Consumer Compliance and Customer Service.
Ralph Fatigate is a Managing Director with Alvarez & Marsal Financial Industry Advisory Services, with more than 35 years of regulatory and financial investigative experience.

Mr. Fatigate recently served as a principal at a regional audit and advisory firm. Prior to that, he was a managing director and practice leader for an international accounting and consulting firm, overseeing anti-money laundering (AML) compliance and remediation, regulatory compliance, financial technology, 1414 tax remediation, and mortgage fraud investigations. Over the past several years, Mr. Fatigate has led and managed many of the most complex BSA/AML/OFAC regulatory remediation projects in the nation. He has expert knowledge on regulatory expectations for BSA/AML/OFAC compliance and significant involvement with automated applications for transaction monitoring and OFAC screenings. Ralph has also developed and implemented OFAC policies and procedures designed to minimize the risk of OFAC violations along all banking business lines. Mr. Fatigate has managed a review SWIFT payment instruments in order to identify any misleading information that would cause an OFAC violation.

Mr. Fatigate is the former Director of Financial Crimes & Investigations at the New York State Banking Department, where he was responsible for the AML/BSA examination process for all state-regulated financial institutions. Additionally he was the Inspector General Liaison for the Department. He also served as the interim Co-Director of the Frauds Investigation Division at the New York State Insurance Department and is the former Commissioner of Police for the City of Mount Vernon. As a police officer and Police Commissioner Mr. Fatigate coordinated numerous harassment allegations both internally and externally. Several of these investigations were ultimately settled in court proceedings.

Soon after September 11, 2001, he worked with federal law enforcement officials in Washington, D.C. and assisted in the development of a data mining system that would identify those who were financially supporting terrorist related activities. He is credited with coordinating and managing some of the large money laundering investigations in the United States. He has worked with local, state and federal prosecutors and assisted in the prosecution of several entities and individuals suspected of laundering funds.

Mr. Fatigate has been a speaker at numerous professional conferences and has provided training for domestic and international groups as well. He has worked alongside the FDIC, OCC and various state regulatory agencies on money laundering, fraud and industry standards issues.

His expertise includes the development of numerous training guides for the Bank Secrecy Act and U.S. Patriot Act reviews. In addition, he has experience providing opinion testimony for Grand Jury proceedings on banking policies and procedures.
Donna DeMartino is a Senior Director with Alvarez & Marsal’s Dispute Analysis & Forensic Services in New York where she is currently the lead in the BSA/AML and Compliance Technology Service Line. She brings more than 20 years of management consulting experience in leading and managing large, complex technology implementation efforts, investigations, BSA/AML Look Backs and Forwards and has supported compliance, forensic, dispute and quarterly audit projects.

Ms. DeMartino has spent more than 14 years focusing on regulatory and compliance engagements within the financial services industry, specifically banking and brokerage. While she specializes in compliance related technologies, such as interdiction (OFAC), transaction monitoring applications, case and SAR management systems, she also has in-depth expertise in the policies and procedures that are captured in the business rules within the compliance’s technology infrastructure (i.e., dynamic risk scoring, customer and enhanced due diligence, wire transfer transactions, e-payments, etc.). Moreover, she also has practical experience with many of the leading transaction monitoring software and OFAC applications available on the market today (i.e., AMLManager, Actimize, Wolters Kluwer, Mantas, SAS, Yellow Hammer, Patriot Officer, Safe Banking Systems, Bridger, etc.).

From a project management perspective, she has provided management oversight to customer remediation efforts, transaction monitoring reviews and assessments, gap analysis, sanction reviews, work flow and case management product selections, testing, refinement and implementations. In addition, she has assisted clients in calibrating their thresholds and settings within the compliance technologies to accommodate enhancements and augmentations made to the financial institutions’ business models. Moreover she has built strong working relationships with the major vendors in the compliance space.

Prior to joining A&M, Ms. DeMartino was a Senior Manager in Enterprise Risk Services Group at Deloitte & Touche where she developed a series of fraud detection modules for the firm’s largest audit clients. She was also a Senior Manager in the Analytic and Forensic Technology group in Deloitte’s Financial Advisory Services practice and Deloitte Consulting.

Prior to Deloitte, Ms. DeMartino was with Pinkerton Consulting and Booz Allen & Hamilton, where she was responsible for managing a number of application development efforts, providing business improvement and IT strategy expertise for the Financial Services Sector.

Ms. DeMartino earned a dual bachelor’s degree in arts and sciences from Syracuse University with honors. She is also a certified anti-money laundering specialist. Over the years, Ms. DeMartino has authored white papers addressing technology relative to transaction monitoring, know your customer and enhanced due diligence, risk modeling and Look Backs. She has also presented her viewpoints as a guest speaker on Compliance technologies at conferences within the United States.
Theresa Baker-Smith is a Director with Alvarez & Marsal Financial Industry Advisory Services in Youngstown, Ohio. She specializes in the Financial Services Industry. Her primary areas of concentration are AML/BSA management.

With more than 25 years of banking experience, Ms. Baker-Smith has held senior management positions in Internal Audit, Corporate Compliance and Corporate Investigations/Due Diligence. Her previous experience includes the implementation of the Corporate Investigations & Due Diligence team for Sky Financial Group, Director of Corporate Compliance and over ten years in Internal Audit including the Director position for five years. Her roles have involved working directly with Executive Management, Board of Directors and regulatory examiners.

Prior to joining A&M, Ms. Baker-Smith spent over three years with TD Bank near Portland, Maine, where he/she most recently served as Senior Vice President, Director of AML/BSA Compliance. While at TD Ms. Baker-Smith managed the personnel and resources of the AML, BSA, CIP, EDD and OFAC teams. She was responsible for the oversight of the AML/BSA programs for the affiliates of the corporation including TD Bank, N.A., TD Bank USA, N.A., TD Wealth Management Services, Inc. and TD Insurance. Her key accomplishments during her tenure at TD included the implementation of SAS transaction monitoring software, the development of the AML Department and Line of Business Quality Control Program; a Technology & Analytics team and Enhanced Due Diligence program. She also managed the integration of Commerce Bank and TD Banknorth, N.A.

Ms. Baker-Smith earned a Bachelor of Science degree in Accounting and Marketing from Clarion University of Pennsylvania. She has been certified as a Certified Public Accountant (CPA), Certified Anti-Money Laundering Specialist (CAMS) and Certified Fraud Examiner (CFE). She is a member of ACAMS, ACFE, AICPA, OSCPA and a former member of the Pittsburgh and New England chapters of the IAFCI. Ms. Baker-Smith has been a speaker for a number of professional organizations and an Instructor for the Western Pennsylvania FBI Academy. She also completed the Penn State University Executive Management Program and the BAI National Compliance School in Norman, Oklahoma.
Peter Kwan is a Director in the Forensic Technology & Security Practice at Alvarez & Marsal.

Currently, Mr. Kwan is working on a BSA/AML technology assessment for a large Latin American bank in Mexico. While at A&M, he has also helped other clients with BSA/AML technology assessments, systems validations, as well as on regulatory mandated Lookbacks to detect suspicious transactional activity and OFAC screening reviews.

Mr. Kwan specializes in the anti-money laundering industry, where he has assisted global financial institutions in the following areas:
- Implementation of interim transaction monitoring systems and case management tools
- Design & execution of search tools to perform watch list (OFAC, SDN) keyword searches
- Targeted transactions detection for Suspicious Activity Reporting
- Data modeling, database development, data analysis, and reporting for look-back engagements
- Scenario and threshold optimization of customized transaction systems

Prior to joined A&M, Mr. Kwan worked in the Data Management group at a Big Four Accounting firm. His client work focused primarily on Anti-Money Laundering projects for financial institutions based in the US, South America, and Asia.

Mr. Kwan has designed data matching techniques to test for the existence of OFAC and High-Risk Geography keywords within raw wire remittance and transactional information working on-site for a major Japanese bank.

Mr. Kwan has implemented interim tools to perform multiple 6-year, retroactive customer risk-rating and transactions analysis for South-American banking clients under scrutiny from the Office of the Comptroller of Currency (OCC).

Mr. Kwan has utilized data modeling and normalization techniques for the creation of a "single" customer view for the risk re-assessment of a Regional Bank’s customer base.

Mr. Kwan received a Bachelor’s degree in Computer Science from Binghamton University. He has also received his certification as an Anti-Money Laundering Specialist from the ACAMS organization.
Tony de la Mora is a Director with Alvarez & Marsal Financial Industry Advisory Service (FIAS) in Houston, with more than 19 years of regulatory compliance and risk management experience.

He has extensive experience in case management (profile alerts, investigations, quality control, currency transaction reports and suspicious activity reporting); risk management (initial due diligence; extended due diligence); fraud prevention detection and investigations; law enforcement inquiries (domestic and international); high risk accounts; custodian of records; board of directors’ compliance training; international banking; and serving as a liaison between both U.S. and foreign government regulators.

Mr. de la Mora has served in different capacities within different financial institutions, including chief risk officer; chief compliance officer; Bank Secrecy Act officer; an office of foreign assets control officer; corporate security officer; and privacy officer. He has managed up to 200 employees.

Mr. de la Mora earned a bachelor of arts degree in cultural anthropology at Instituto de Antropología y Ciencias Sociales, México City and a bachelor of science degree in general science from the Instituto Tecnologico Y de Estudios Superiores De Monterrey (ITESM), Monterrey Institute of Technology for Higher Studies; Mexico City. He received certification from Regulatory Compliance School, Emory University, Atlanta in 2005.

He is a Certified Fraud Examiner (CFE), a Certified Anti-Money Laundering Specialist (CAMS) and a Certified Financial Crimes Investigator (CFCI). In addition, he is a member of the American Bankers Association, the American Red Cross, the Community Emergency Response Team (CERT) and has served on the Fraud Advisory Committee of the U.S. Attorney's Office.

Mr. de la Mora received a Distinguished Service Award from the State of Arizona's District Attorney General and special recognition from the Mayor of Tempe, AZ for his comprehensive service to the community.