The Top 10 Risks For Mobile Payments

The Risk Management Group
March 2012

Sponsored by:

Lavastorm Analytics is a global business performance analytics company that enables companies to analyze, optimize, and control the performance of complex business processes, including financial, operational, and customer experience processes.

The company’s Lavastorm Analytics Platform offers a new, agile approach to fraud management and revenue assurance and is used by thousands of business and IT professionals at more than 50 CSPs worldwide. The platform’s discovery-based, audit analytic capabilities provide users with self-service analytics, visualizations of process/performance issues, continuous monitoring and auditing, and case management capabilities for issue resolution.

For more information please visit: www.lavastorm.com
The Top 10 Risks For Mobile Payments

MOBILE MONEY

Electronic money is now a well established means of exchange. Credit card balances and payments are one form of E-Money, however, the emergence of new forms, such as Mobile Money and Mobile Payments, are increasing consumer interest and usage. Their importance to operators is increasing as a result.

As operators transition from being bearer service providers into providers of a mix of services that includes payments, mobile money and other banking services, their regulatory burden will increase exponentially. See Figure 1.
Figure 1  Operator’s Evolving AML/CTF Regulatory Burden

KEY MOBILE PAYMENT RISKS

Mobile payment models introduce a number of new risks for operators. As Figure 1 illustrated, the entry into a heavily regulated financial services sector will place demands on operators to address a range of preventative and analytical challenges. The highest profile issues anti-money laundering (AML), countering terrorist funding (CTF or CFT) and tax evasion and we will therefore provide a little extra background on these topics here.

M-PAYMENTS AML, CTF AND TAX EVASION CONSIDERATIONS

While mobile payment challenges are relatively new, there are existing models in the financial services sector that illustrate when and to what extent a communications operator must start to comply with AML (anti-money laundering) and CTF (countering terrorist funding) regulations. Not surprisingly, the greater an operator’s involvement in the delivery of financial services the greater the burden of AML and CTF regulation will be. As potentially innocent participants in money laundering cases, regulated firms stand to have their reputations tarnished when money laundering
cases are proven, and they may also be judged to be non-compliant with regulations governing the sector, resulting in punitive action.

**What is money laundering?**

Money laundering refers to any action deliberately taken to conceal the proceeds of crime. It differs from tax evasion in the sense that the money is considered tainted at the outset, and the goal of those engaged in money laundering is to process these funds so as to make them appear legitimate, or clean. Typically, money laundering cases involve a number of transactions between businesses setup for the purpose, often via banking houses that may be unaware of what is being done.

Classic money laundering is a three step process, although it is important to recognize that each case will be unique:

- **Placement.** The illicit funds are introduced into the financial system, for example via a fake retail operation that accepts cash payments but which delivers no goods of value.
- **Layering.** This involves a series of complex financial transactions, typically via numerous accounts in several different institutions and countries, intended to conceal the source of funds and confuse investigators.
- **Integration.** This is the final step whereby the laundered funds are passed to the final beneficiary.

**Responsibility for anti-money laundering controls**

In order to comply with international AML regulations, regulated institutions are required to implement anti-money laundering controls internally. These include Customer Due Diligence (‘CDD’) controls, applied when new accounts are being opened, as well as ‘Know Your Customer’ or ‘KYC’ arrangements and Suspicious Transaction Reporting (‘STR’) mechanisms.
The top 7 requirements for effective AML

A number of leading international financial institutions have come together to form the Wolfsberg Group, which focuses on defining and promulgating effective anti-money laundering guidelines that complement the existing regulatory framework. These are behind a transition by most jurisdictions to a risk-based AML approach which calls for segmentation of suspected cases based on country risk, customer risk, services risk and transaction risk, to arrive at an overall risk score per event.

Some of the key components of an effective anti-money laundering programme as recommended by us are:

1. Training of staff
2. Risk scoring of customer details
3. Profiling & trending analysis routines to detect behavioural deviations
4. Automated alerting & case management mechanisms
5. Suspicious transaction/activity reporting procedures
6. Data retention & audit capabilities to support post-event investigations
7. Case management & investigation capabilities designed to identify perpetrators

Money Laundering Red Flags for Operators

1. **Transaction details:** automated analysis at record level, similar to FMS analysis today

2. **Documentation:** manual analysis of the documentation related to accounts, identity or transactions

3. **Parties involved:** identities and background of parties involved (e.g. PEP analysis)

*Figure 3  Common Money Laundering Red Flags*

Additional controls often include:

- **Public record searches**
  - Media and Internet searches, including blogs and social media sites
  - Corporate records and other relevant business information searches (e.g. bankruptcy or insolvency records and litigation findings
  - Regulatory filings
  - Records on public procurement tenders
  - Sanctions and watch lists

- **Discreet enquiries (normally outsourced)**
  - For red flag investigations
  - To fill gaps in public records
  - To balance potentially biased media reporting
Demonstrating due diligence

Every regulated firm is required to have its own money laundering officer (MLRO) who is responsible for ensuring that the firm establishes and maintains effective systems and controls for compliance with the various requirements and standards under regulatory systems, and for countering the risk that the firm might be used for financial crime. The MLRO sets compliance policies and delegates responsibilities for effective risk rating and monitoring of individuals and transactions to operational teams. The emphasis is thus on the experience, training and skills of the operational teams and the effectiveness of the firm’s internal processes and controls for effective compliance management.

Countering terrorist funding

Terrorist funding is conceptually very similar to money laundering, in that the sources and final destinations of funds may be concealed, but it has some very important differences that make it much harder to detect:

- The movement of terrorist funds generally precedes the commission of the terrorist act, whereas money laundering occurs following the commission of a crime.
- The sums required to fund a terrorist cell are typically only a small fraction of those moved in most money laundering cases.

Consequently, except in instances where customer due diligence procedures have triggered alarms, monitoring of terrorist funding is often either intelligence led or post-event; “right of bang” in security parlance. Therefore, the secure retention of both customer and transactional data is crucial in such cases, and represents the main mechanism for ensuring compliance.

The business repercussions of failing to prevent ML and TF

Failure to establish suitable and effective controls, processes and policies would have serious and damaging repercussions to a regulated firm. It is an offence, potentially leading to prison terms for responsible staff and/or fines, for firms to fail to comply with anti money laundering regulations in most jurisdictions. Serious breaches are also widely publicised by regulators and can have far reaching and long term effects on an organisation’s brand and reputation.

TOP 10 M-PAYMENT RISKS

The following table summarises the top ten mobile payment risks that need to be addressed by fraud, risk, credit or security teams within operators and regulated firms.
<table>
<thead>
<tr>
<th>M-PAYMENT RISK</th>
<th>REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud against subscribers (e.g. possible theft of their balances through staff involvement or technical means).</td>
<td>The store of value can sit on the phone (handset, SD card or SIM) or in a location across the network. If it is on the phone, how is it protected? If it is elsewhere, how are the communications protected against interception and manipulation? How is the remote store protected?</td>
</tr>
<tr>
<td>Assuming control of someone else’s account via a man-in-the-middle attack.</td>
<td>Researchers at Cambridge University and elsewhere have reported(^1) that fraud is achievable under the current EMV security standards.</td>
</tr>
<tr>
<td>Shoulder surfing and device theft, which involves a thief viewing the PIN entered and then stealing the device or card.</td>
<td>For a decade after the introduction of card services, shoulder surfing was the predominant type of card fraud. It provides the main justification for biometric security controls.</td>
</tr>
<tr>
<td>Someone else makes expenditure against a customer’s account or the account is charged more than once for the same purchase.</td>
<td>The public has a widespread concern that contactless payment opens up risks that don’t exist when a card has to be swiped. Whether these concerns are valid or not, they affect take up and therefore the business case for new services.</td>
</tr>
<tr>
<td>Falsely acquiring a line of credit by setting up an account in a false name or in someone else’s name.</td>
<td>Using a false identity to obtain a line of credit or using false information to obtain more credit than the situation warrants is currently a widespread problem and this will no doubt continue for the foreseeable future.</td>
</tr>
</tbody>
</table>

\(^1\) [http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf](http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf)
<table>
<thead>
<tr>
<th>The Top 10 Risks For Mobile Payments</th>
</tr>
</thead>
</table>

| Repudiation fraud by subscribers (i.e. “I didn’t make that transfer – my phone was stolen.”) | Banks and EMV providers have traditionally tried to use their Terms and Conditions to place the burden of proof on the shoulders of the customer. Regulators are increasingly unwilling to allow these arrangements to continue, and the burden of proof is again being shifted to the providers. |
|-------------------------------------|

| Coercion of customers to make payments against their will, for example by thugs at an ATM. | Existing systems tend to be reactive, that is they react to customer’s reports after the event. Most systems cannot report or detect coercion in real time. |
|-------------------------------------|

| Use of MM for layering transactions during money laundering or for terrorist funding purposes and other organised crime or corrupt payments. | Mobile money solutions can be exploited by generating large numbers of low value transactions, possibly using automated tools or software. This type of attack is difficult to police and so regulators tend to set low maximum transaction values to minimise this risk thus inconveniencing honest users of the payment system. The big question will be whether regulators and providers are able to maintain those low transaction thresholds in the face of market pressures. |
|-------------------------------------|

| Internal denial of service attacks (Cybercrime). | A team of attackers using the service may attempt to swamp or flood a mobile payments system with large numbers of very small transactions. |
|-------------------------------------|

| External denial of service attacks (Cybercrime). | This is a risk with all electronic payment solutions as demonstrated by the attacks perpetrated by Anonymous. |
CONCLUSIONS

Every new technology or service triggers a cascade of new risks, vulnerabilities, control requirements, business process changes and training needs. Mobile payments will be no different and we need to focus our attention on the topic at an early stage. What does make mobile payments special is the fact that they mark the convergence of financial services (FS) and telecommunications, thus introducing FS fraud and IT risks to telecoms and telecoms technical and fraud risks to FS.

Regulated firms, telecom operators and vendors all need to pay careful attention to these developments as the impact of payments frauds and risks can extend far beyond the corporate balance sheet.

ABOUT TRMG

The Risk Management Group has specialised in the delivery of training and consultancy on high tech fraud for leading firms worldwide for over a decade. For more information on TRMG, visit www.trmg.biz.