



VISA COMMERCIAL SOLUTIONS 

VISA INTELLILINK COMPLIANCE MANAGEMENT WHITE PAPER

Converting commercial payment data into critical, cost-saving intelligence.

Employee fraud is a multibillion-dollar problem that affects both government agencies and private-sector companies. A 2008 report by the Association of Certified Fraud Examiners showed that fraudulent activity costs U.S. businesses \$994 billion dollars each year.¹

Most fraud is conducted by first-time offenders, so background checks do not reveal potential problems. Studies also show that theft generally begins small, and develops and grows over time as the employee becomes bolder and believes that they will escape detection. It generally takes about 18 months to uncover a fraud incident.²

Electronic payment and commercial card programs offer a first step in deterring fraud. Commercial payment solutions offer a number of inherent controls that card program managers can use to lessen the opportunity for the misuse of funds. Internal audits and Issuer reporting can add another layer of protection.

However, there is still a need for more effectual tools to measure and audit compliance within commercial payment solutions. What's needed is a continuous and cost-effective way to monitor all commercial card activity. Card program managers also need the transaction information presented in a way that helps them act in a timely manner to reduce instances of fraud and non-compliance.

This paper looks at:

- Why it's critical to monitor and identify potential misuse, abuse and waste
- How organizations are currently monitoring adherence to commercial payment solution rules
- What the emerging class of oversight and detection tools offers and how they facilitate compliance management

¹2008 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2008.

²<http://www.thethrivingsmallbusiness.com/articles/employee-fraud/>, February 2010.

The Hidden Costs of Fraud and Misuse

Misappropriation of funds costs organizations billions of dollars every year. And this is only part of the impact fraud can have on an organization. Costly litigation, loss of assets, damage to reputation, loss of consumer trust and plummeting stock prices may follow a fraudulent incident.³

Fraud happens with all types of payment methods from theft of petty cash to sophisticated accounting schemes. Electronic payment solutions can enable an organization to reduce fraudulent activity with the built-in controls they provide. Yet even with rigorous enforcement of these controls and the organization's usage policies, the possibility for fraud and other types of misuse still exist. This can lead to lost revenue opportunities that diminish the savings and benefits of the commercial payment solution through:

- An inability to negotiate favorable pricing if spend is not directed at preferred vendors
- A reduction of volume incentives that may be available on the card program
- Difficulty assessing total departmental spend when transactions occur through multiple or non-card sources (e.g., purchase orders, cash)
- Delayed payment while questionable transactions are investigated

Heavily publicized incidents of fraud and misuse may create a perception that delinquencies are common within commercial card programs. Research tells quite a different story, however. A 2010 RPMG Research study found that purchasing card misuse accounted for an average of \$140 for every \$1 million—less than one tenth of 1%—of card spend and was less in government agencies than private sector companies.⁴

A 2006 RPMG study also found that travel card fraud on average accounts for less than 8/1000 of 1% of travel card spending. This is the equivalent of \$80 of fraud for every \$1 million of travel card spending.⁵

These studies suggest that misuse of commercial card payment solutions is not a rampant problem. Yet organizations need to remain vigilant in dissuading misuse to reap the greatest benefits and minimize the negative consequences.

How Card Programs Can Help Control Misuse and Abuse

Commercial cards are equipped with inherent characteristics that can improve oversight and control of spend. Establishing usage policies that limit where, how and how much can be spent on the card by any one employee can make these controls more effective. Strict enforcement of the organization's policies is also essential to limit abuse and out-of-policy spend.

2.7 billion is lost everyday by U.S. businesses to employee fraud from all types of payment methods.¹

³"Private Equity Review, First Quarter 2010," RSM McGladrey, Inc., 2010.

⁴Palmer, R. and M. Gupta, "2010 Purchasing Card Benchmark Survey," RPMG Research, 2010.

⁵Palmer, R. and M. Gupta, "2006 Corporate Travel Card Benchmark Survey," RPMG Research, 2006.

Electronic payment solution controls include, but are not limited to:

- Authorization controls, including blocking spend at certain merchant categories
- Spending limits
- Chargeback capabilities
- Real-time fraud scoring
- Detailed transaction reporting

These and other built-in restraints may account for why satisfaction levels for commercial payment cards are higher than all other payment methods. A 2009 survey found that 91% of U.S. respondents reported satisfaction with commercial cards as a method of making payments. Respondents also indicated that their commercial card usage would likely continue to increase. More than 60% of respondents anticipated shifting an additional 20% of spend to their commercial payment cards in next 12-18 months. Nearly 55% anticipated reducing their organization's reliance on checks as a form of payment.⁶

While these intrinsic properties of commercial payment solutions can make them a safer payment form than paper-based methods, additional tactics can contribute to a climate of oversight and control.

Types of Commercial Payment Solution Misuse

Non-compliance with an organization's card usage policies erodes the process efficiencies and cost savings of the payment solution. This out-of-policy spend can result from a lack of knowledge of corporate policies (e.g., purchasing from an unauthorized merchant) or from intentional abuse (e.g., purchasing items for personal use).

Examples of transactions that should trigger audit consideration include those made by cardholders who:

- Purchase with restricted merchants or MCCs (merchant category codes)
- Withdraw cash on the company card with no associated travel or on non-work days (to help create a cash float)
- Use convenience checks excessively to withdraw against the card's limits
- Make out-of-policy travel arrangements
- Transact with only one merchant (the cardholder may be directing funds from the card to a shadow business they have set up)
- Split large purchases into several transactions (may be an attempt to circumvent card limits or expense thresholds)
- Make multiple purchases of even dollar amounts (e.g., \$100, \$250), which could

More than
60% of
respondents anticipated
shifting an additional
20% of spend to their
commercial payment
cards in next 12-18
months.⁶

⁶Global Cash Management Survey, commissioned by Visa Inc. and conducted by Survey.com, 2009.

signal an attempt to exceed cash limits by getting funds from a merchant or financial institution as a charge, rather than from an ATM

- Suddenly begin using their card more frequently or for higher dollar amount purchases than usual

Mitigating Abuse through Traditional Methods

Organizations use several strategies to ensure compliance and limit the amount of unauthorized activity on their commercial cards. These range from the guidelines established during program implementation to ongoing audits of card activity.

The following table lists some common tactics⁷—including the program controls discussed above—as well as the limitations they present.

Strategy	Description	Limitations
Program Controls	<ul style="list-style-type: none"> • Includes guidelines for card issuance and usage, such as credit limit and velocity controls, merchant blocking, approval procedures and more • Should include a clear definition of each participant’s role—from program administrators to cardholders—to minimize the gap in accountability • Set up as part of the program design • Should be reviewed regularly and modified as needed 	<ul style="list-style-type: none"> • Only as effective as the ability to enforce the controls • Provides no visibility into whether the controls are actually working • Allows cardholders to exploit ineffective procedures until the controls in question are discovered/modified
Reconciliation Procedures	<ul style="list-style-type: none"> • Matches activity on card statements to documentation (receipts, purchase records, etc.) • Makes it easier to spot unauthorized activity that occurred during the billing period 	<ul style="list-style-type: none"> • Relies on cardholder honesty and/or approving manager supervision in the matching process • Must be reviewed in a timely manner to be effective • Requires manual effort that may be impractical for large organization with high transaction volumes
Internal Auditing	<ul style="list-style-type: none"> • Can include process audits where the effectiveness of program controls is reviewed and transaction audits • Can be conducted at random and regular intervals • Should be conducted more often for high risk areas (high dollar amounts, large number of transactions by one cardholder, etc.) 	<ul style="list-style-type: none"> • Only conducted periodically • Only monitors certain transactions or controls • May be months/years between the questionable transaction and its detection • May involve a team of auditors that is larger than the card program management team • May require more sophisticated data mining tools than the organization can provide
Internal Reporting	<ul style="list-style-type: none"> • Can be performed on a regular schedule (daily, weekly, etc.), as well as ad hoc basis • Should review standard indications of suspicious activity, such as declined transactions, disputed charges and out-of-policy activity 	<ul style="list-style-type: none"> • Only monitors certain transactions • Can only search for what is already known • Data must be compiled from multiple sources, increasing the probability of inaccuracies

Strategy	Description	Limitations
Issuing Bank Reporting <small>(through Electronic Access System (EAS) reports)</small>	<ul style="list-style-type: none"> Can offer spend reports that help managers analyze individual cardholder spend and overall spend activities Can offer line-item detail (through Level III data) for greater visibility into card activity 	<ul style="list-style-type: none"> Generally does not monitor 100% of transactions May not offer the full range of reports needed by the organization

It has been estimated that nearly two-thirds of misuse incidents are identified through these various methods.⁷ Detecting the remaining one-third of the occurrences of unauthorized activity may require more robust management solutions and continuous access to metrics that allow card program managers to act before the non-compliance or fraud becomes widespread.

Emerging Compliance Management Tools

Uncovering instances of misuse not easily detected by traditional methods can be a costly and arduous task, compounded by the sheer volume of information that is created with each transaction. Cardholder name, number, merchant name, MCC, purchase amount and date are a mere fraction of the data captured each time a commercial payment solution is used. Multiply this by the number of cardholders and number of transactions each cardholder makes per month and it is clear that intensive data mining is needed to drill down through these volumes of information and sort the data in a meaningful manner.

The marketplace is responding to this need with sophisticated new tools designed to allow organizations to reap full value from their commercial payment solutions. Using cutting-edge data mining techniques, this new class of compliance management applications is being implemented by leading organizations to:

- Detect and deter fraud and waste
- Enforce policies and procedures
- Deliver financial justification for expanding the card program, thereby delivering greater efficiencies and savings to the organization
- Fulfill government reporting requirements

Key Attributes

While each provider takes a unique approach to compliance management, there are a number of attributes that can be found across many solutions. The following lists the intended benefits these features present.

Ongoing Monitoring (continuous or as needed)

- Uncover unforeseen risks and opportunities for operational improvement
- Accelerate the ability to act on questionable transactions
- Remove the need for time-consuming, costly manual efforts

The marketplace is responding to this need with sophisticated new tools designed to allow organizations to reap full value from their commercial payment solutions.

⁷Fraud Prevention and Detection: Establishing and Maintaining a Purchasing Card Program with Adequate Management Controls to Prevent Fraud, Misuse and Abuse, NAPCP, January 2004.

Transaction Evaluation (all or sample)

- Detect questionable or out-of-policy transactions immediately
- Provide a more complete picture of patterns of use
- Eliminate spot checking (only when all transactions are evaluated); no transaction falls through the cracks

Data Integration

- Pull information from multiple systems and sources
- Provide a more holistic view for greater insight

Standard and Ad-hoc Reporting

- Allow organizations to run reports of the most benefit to them
- Permit customization of report types

Dashboard Visibility

- Give managers a snapshot of program performance metrics
- Provide a central location where users can easily access the level of information they need

Transaction Scoring

- Use algorithms to search for anomalies, including those that would not typically be detected via known rules
- Leverage interactions between various transactional and cardholder attributes
- Provide a view of usages patterns and trends

Automated Alerts

- Proactively flag non-compliant transactions
- Give card managers timely access to exception reports

Behind-the-firewall versus SaaS Solutions

Today's class of compliance management solutions is divided between traditional delivery methods and the Software-as-a-Service (SaaS) model.

Behind-the-firewall applications can offer a number of benefits, including:

- Flexibility to customize to each client's requirements and incorporate requests for enhancements sooner
- Greater control over the content

Worldwide revenue for the SaaS market is forecast to rise from \$13.1 billion in 2009 to \$40.5 billion in 2014—a compound annual growth rate of over 25%.⁸

⁸Worldwide Software as a Service 2010-2014 Forecast: Software Will Never Be the Same, International Data Corporation, June 2010.

SaaS solutions can offer:

- Lower up-front costs and total cost of ownership
- No ongoing maintenance or upgrade installations
- Accelerated deployment
- Greater ability to scale and meet changing business needs

SaaS compliance management solutions also allow all users to work with the same and most recent version available, thus eliminating potential conflicts. This can be of critical importance, especially if card program operations are geographically dispersed.

An Overview of Visa IntelliLink Compliance Management

Visa IntelliLink Compliance Management is a web-based solution that provides intelligent assistance for optimal card program management. It converts transaction data into information program managers can use to minimize and deter misuse and abuse and maximize savings. Using the SaaS delivery model, it can be deployed quickly at a lower cost than traditionally delivered software applications.

The solution is designed to give organizations a more detailed and robust way of looking at their commercial payment program data, aiding in the detection and mitigation of questionable behavior. In-depth and timely reporting can facilitate remediation of out-of-policy spend, while producing an electronic audit trail that provides a system for recording all actions taken. These deeper levels of data complement existing card management and Issuer reporting systems for a 360° view of commercial payment solution activity.

Visa IntelliLink Compliance Management's monitoring of card usage in minute detail also helps card program managers ensure that their commercial payment programs are achieving optimal savings and benefits by operating according to their organization's policies and regulations. The application's range of services includes:

- Analytics and investigative reporting, including drill-down dashboard capabilities to measure program performance
- Misuse and abuse detection, including a neural-network transaction scoring system that can detect questionable behavior not easily apparent to the human brain
- Reporting that enables program and regulatory compliance
- Self-service administration

Visa IntelliLink Compliance Management has been validated by a third party as meeting the requirements of Section 508 of the Americans with Disabilities Act and the Payment Card Industry Data Security Standards (PCIDSS).

These deeper levels of data complement existing card management and Issuer reporting systems for a

360° view of commercial payment solution activity.

Modularity Facilitates Customization

Visa IntelliLink Compliance Management is a component-based tool. This modularity provides greater agility for responding to the continuous changes required to meet shifting business needs, while accelerating the integration of technological advances. Modularity also means the solution can be tailored to each organization's needs, whether an enterprise, domestic or international government agency, higher-education organization or other entity.

The modules work together to give program managers different ways of looking at their data. The Rules module automatically compares every transaction to a strong suite of industry-standard rules, plus those added by the organization. The Predictor module offers neural-network scoring, which allows the detection of questionable behavior that is not immediately apparent to the human brain. This module also learns continuously from usage data and refines the results in an effort to reduce the number of false positives.

All suspect transactions flagged by the sophisticated data mining capabilities of these and other modules are sent to the Compliance module for review and remediation. The Compliance module helps enable managers to take action and provides a system of record for the actions taken, thereby offering a more complete, easily accessed electronic audit trail.

Other modules work to simplify reporting, determine the statistical likelihood of an undesirable occurrence, help with program administration, sourcing analysis and more.

Real Results with Compliance Management

Visa IntelliLink Compliance Management can be effective in identifying questionable spend in numerous categories. A review of programs that had implemented Visa IntelliLink Compliance Management at the time of sampling demonstrated the following*:

46% reduction in restricted MCC spend⁹

28% decrease in spend on weekends⁹

13% drop off in split transactions⁹

*The percentage decreases were based on the proportion of transactions made in the listed categories.

⁹The estimates of savings were derived from a sample of 33 card programs' purchase and travel card transactions for MCC spend, and purchase card transactions for weekend spend and split transactions. The percentage decreases were based on the proportion of transactions made in the listed categories between Time Period A (December 1, 2007 through September 30, 2008) when the programs had not deployed the Visa solution and Time Period B (December 1, 2008 through September 30, 2009) when the programs had deployed it.



Summary

Minimizing fraud and non-compliant spend is essential to the success of a commercial payment solution and to protect organizations from financial losses, costly litigation and loss of reputation that can negatively impact stock prices. The internal controls inherent in commercial payment solutions, as well as traditional methods of auditing and ad-hoc reporting add layers of accountability and create a cultural climate of control within the organization. Yet auditing and reporting can be time-consuming and costly to perform, error-prone due to their manual nature and incomplete in their monitoring of the program's performance.

State-of-the-art data mining provides the detailed level of review and reporting needed to manage today's commercial payment programs. The new class of compliance management programs offers ongoing transaction monitoring that can provide managers better insight into their card program's performance and intelligence that can be acted upon to quickly detect and discourage fraud, waste, loss and abuse.

Visa IntelliLink Compliance Management offers advanced data mining capabilities in a zero-footprint, web-based environment. This intuitive solution is designed to complement existing card management systems in a cost-efficient software-as-a-service model and component-based design.

By converting transaction data into critical intelligence, today's sophisticated compliance management applications—including Visa IntelliLink Compliance Management—are designed to allow organizations to derive the greatest value and cost savings from their commercial card programs.

For more information about Visa IntelliLink Compliance Management, please contact your commercial banker or visit visa.com/intellilink.