CHASE

J.P.Morgan

COMMERCIAL CARD

FRAUD MANAGEMENT IN COMMERCIAL CARDS: Proactive Vigilance and Collaboration Required

INTRODUCTION

With their numerous benefits, commercial cards, which include corporate travel and entertainment (T&E) cards, purchasing cards, fleet cards and more, are well-established vehicles for business-to-business (B2B) payments, particularly in North America. Yet, news about data breaches and card fraud can unnerve even stalwart card supporters. There is no denying that fraud can and does happen, originating from various sources, both internal and external.

At the broadest level, card fraud is the unauthorized use, or attempted use, of a payment card. The incidence of commercial card fraud is far lower than the incidence of fraud on consumer cards, and it is lower than the incidence of corporate check fraud. The 2015 AFP Payments Fraud and Control Survey reveals that paper checks are the payment type most susceptible to fraud attacks even as their overall use continues to decline. Check fraud also accounts for the largest dollar amount of organizations' financial loss due to fraud. Credit/debit cards are the second most popular vehicle for payments fraud; 34% reported fraud attempts via credit/debit cards in 2014, down from 43% in 2013.[1]

Fraud management in the financial services industry has always been a matter of trying to stay one step ahead of the fraudsters. This is a great challenge due to the relentless and global pursuit of ill-gotten gains by an amalgam of criminals. As a regulated financial institution, JPMorgan Chase is required to develop, maintain and constantly update the processes, procedures and systems used to manage risk across our banking entities and products, including commercial cards. Regulatory compliance is of course non-negotiable. A substantial part of the equation is to maintain our reputation as a safe and sound place to help manage the financial resources of the many millions of individuals and companies who place their trust in the institution. JPMorgan Chase also understands that we must accomplish this while creating an optimal experience for our clients, including seamless, uninterrupted service, the protection of information and prevention of potential financial losses through card fraud.

JPMorgan Chase takes the threat of fraud very seriously and devotes numerous resources to prevention. Our commercial card fraud loss statistics, measured as a percentage of card spending, are below the industry average and a far lower rate than the fraud associated with consumer cards. This low fraud rate speaks to the strength of our fraud prevention practices as well as relationships with clients in establishing effective card controls. In this paper we will discuss card fraud in more detail and some of the ways that JPMorgan Chase works to reduce the risk.

[1] Business Wire, http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion fraud/.

Card Fraud Scope and Definition

Card-related fraud is a major challenge around the globe. One industry estimate puts 2014 losses at roughly $16 billion, with the potential to reach $35 billion by the end of this decade. These direct losses are shared by financial institutions, merchants and businesses, so it is a distributed pain that requires collaboration to manage across the industry spectrum. There are also other expenses in addition to the direct fraud loss, including costs of administering the post-loss process, ongoing prevention, and investigating the fraudsters for potential prosecution. In the United States the challenge has been somewhat greater because the fraud-resistant EMV/chip card technology is only in process of being deployed by banks and merchants, likely requiring about two more years to be fully implemented across the market.

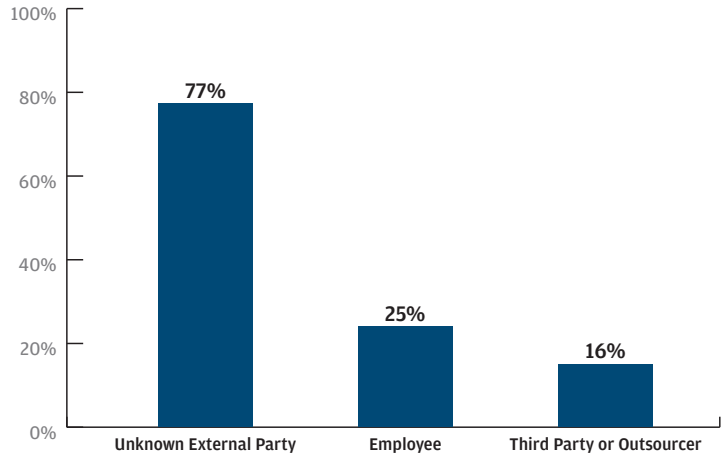
Unlike consumer fraud, commercial card fraud can originate internally when an employee cardholder uses the card for personal gain or shares with others for that purpose. The same AFP survey (with 741 responses from organizations of all types and annual revenue ranging from under $50 million to more than $20 billion), indicates that among organizations whose commercial card programs were subject to fraud, 25% reported fraud perpetrated by their own employees.[2] A separate source of internal fraud arises from policy violations whereby an employee makes business purchases that do not follow the company's rules. Examples include purchasing from a supplier that has not been approved, buying unnecessary or unauthorized goods, and purchasing higher volumes than allowed.

More common, though, is external fraud involving a lost, stolen, or counterfeit card and/or stolen account information (see Exhibit 1). External fraud categories also include situations where the card(s) is not received, somehow intercepted prior to the corporate employee or administrator. An unknown external party was the most common source of fraud found by the AFP Survey, at 77% of incidences. Counterfeit card fraud results from cards manufactured by fraudsters using detailed account information stolen by various means.

Data breaches and the subsequently compromised card accounts have made headlines in recent years, bringing the problem of fraud to the forefront and revealing vulnerabilities that allow it to occur. These are sometimes a result of merchant network vulnerabilities, skimming card information at the point of sale, or even stolen equipment. Breaches also occur through phishing and even more sophisticated credit master processes, where computer-generated account number algorithmic combinations are tested for validity. Indeed, data breaches may help explain the sharp increase in fraud and awareness of it. Fraudsters are certainly mindful of the transition to EMV/chip cards, and have increased their counterfeit card attacks before the opportunity dwindles. Overall, parties involved in external fraud can range from a lone perpetrator to experienced criminal rings.

EXHIBIT 1: UNKNOWN EXTERNAL PARTY IS THE LEADING SOURCE OF CARD FRAUD

Percentage of Organizations That Suffered at Least One Attempt at Corporate or Commercial Card Fraud, by Party Responsible, 2014



Source: 2015 AFP Payments Fraud and Control Survey

[2] This report is issued by the Department of Commerce's U.S. Census Bureau and the Bureau of Economic Analysis.

The JPMorgan Chase Fraud Team Approach

The myriad benefits of commercial card programs of course far outweigh the financial losses incurred through fraud. One way is through overall order processing costs. According to the 2014 Purchasing Card Benchmark Survey Results by RPMG Research Corporation, a purchasing card process is estimated to be $20.38 per transaction, roughly three to four times less expensive than traditional procure-to-pay processes (depending upon the relative efficiency of corporate processes).[3] JPMorgan Chase recognizes, however, that fraud remains a financial risk to our clients, and can also be an invasive experience to an individual cardholder, as well as extremely inconvenient, especially during important business travel circumstances. Therefore we invest a great deal in a comprehensive approach to the prevention and overall management of fraud.

Our approach to managing fraud involves four major sets of ongoing and interrelated activity. (see Exhibit 2). Each operational activity is designed to provide an optimal end-to-end set of standards to prevent fraud, minimize its' effect, reduce negative client impact and establish constant learning inputs for greater effectiveness. The fraud team provides inter-operational feedback, based on established cases, new trends, external agency and industry intelligence, and systems monitoring. In summary these activities are as follows:

- **Strategy –** This group establishes commercial card reduction strategies and tactical approaches, along with optimal fraud monitoring technology used in conjunction with the cards processing systems. They are monitoring internal and external trends, while participating in industry fraud intelligence activities.
- **Prevention –** This group makes operational decisions impacting accounts through a combination of account activity monitoring and cardholder communication. They both prevent fraud and through immediate action, minimize its' financial and client impact if already in process. If JPMorgan Chase suspects fraud, we have a multi-channel communication process to attempt contact with the cardholder. If the cardholder or admin suspects fraud, one of our fraud experts must actually speak with them before taking action to close the account. This minimizes inconvenience before setting corrective action into motion.

EXHIBIT 2: COMMERCIAL CARD FRAUD TEAM OVERVIEW

[3] Association of Financial Professionals, http://www.afponline.org/fraud/.

- **Recovery –** This group manages post-fraud activity, including merchant chargebacks, cardholder and company reporting, network updates and potential threat filings with the FFIEC.
- **Consultation –** This group works directly with program administrators to establish up best practices for external and internal fraud prevention and monitoring. They also work with external law enforcement agencies on case investigations and prosecutorial referrals.

Client Collaboration

In the multiple lines of defense against card fraud, one of the most important elements is the actual set of card program policy decisions enacted by the corporate client. JPMorgan Chase places a high priority on providing our corporate clients with program set-up advice based on industry-leading knowledge and experience to establish appropriate policies. In addition to the proactive fraud monitoring that is provided as part of program, we also place fraud controls directly in the hands of the program administrator through PaymentNet, our online management front end system. The client can easily generate reports to monitor declines, cash advances, and unusual card activity as well as all other account and transaction details. In addition, program administrators can apply credit, velocity, and MCC controls to precisely define allowable transactions and align card usage with chosen internal policies. Our Implementation Associates and Program Coordinators will work with administrators on training and set up so that intended policies are accurately established. However, the client is in control and can subsequently change settings themselves based on internal policy decisions, providing overall contractual limitations are not impacted (for example, corporate credit line).

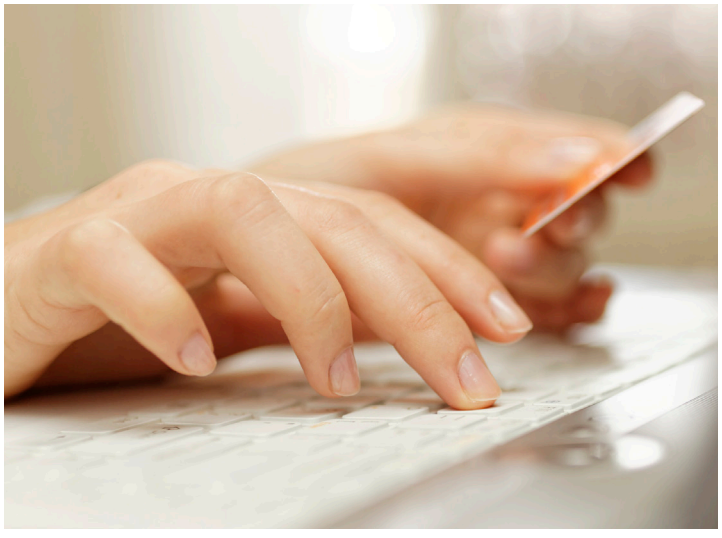
JPMorgan Chase places a high priority on providing our corporate clients with program set-up advice based on industry-leading knowledge and experience to establish appropriate policies.

We remain available consultants throughout the program tenure and will also connect with corporate clients to provide new fraud intelligence as it arises, allowing them to update their program settings if applicable. An example is that our fraud team will provide a detailed fraud consultation walkthrough to client executives and program administrators explaining fraud performance in depth. This consultation includes collaboration with your program administrators to identify and implement ongoing improvements. This ongoing training, communication and two-way collaboration is a hallmark of our approach and an important reason for our strong fraud loss results.

Best Practices

There are numerous best practices for companies to minimize card fraud, both internally and externally. (see Exhibit 3) These can be placed into three general categories:

- **Anti-Fraud Technology Control –** JPMorgan Chase utilizes industry leading fraud detection, scoring, and prevention tools to minimize internal and external fraud. Other solutions, often offered by third-party technology providers, are specific to auditing/transaction monitoring and might accommodate other types of payments, not just cards. The key is to find the correct balance in setting the controls. If controls are too tight, the program may not reach its true potential.



Companies should not overlook the value of conducting a risk analysis and repeating it annually to ensure it evolves along with the card program. Such analysis serves to document the controls and identify potential control gaps. The results should lead to improvements in controls and more effective internal auditing.

- **Prevention –** being effective practitioners involves more than just technology, most often incorporating proper communication. Examples of these may seem rudimentary but should be reviewed.
  - Well-defined roles and responsibilities, such as employee cardholder, manager/approver, program manager/ administrator
  - Separation of duties, especially pertaining to the program manager and provider invoice payments
  - Clear and complete policies and procedures
  - Internal agreements around program policies and consequences of non-compliance
  - Mandatory annual training for cardholders and managers

Companies should not overlook the value of conducting a risk analysis and repeating it annually to ensure it evolves along with the card program.

- **Detection –** one of the largest contributors to internal card fraud and policy violations is poor oversight. Organizations should mandate transaction review by cardholders and their managers at a minimum of once per month. Cardholders are the gatekeepers and should be the first ones to spot potential external fraud, taking the prescribed steps for limiting the impact. Program administrators should also review provided reports (declined transactions, new accounts, closed accounts, system access, etc.) It is also recommended to enact adequate program auditing to evaluate adherence to policies and procedures and the effectiveness of controls.

EXHIBIT 3: COMPANY BEST PRACTICES SUMMARY FOR COMBATING CARD FRAUD

Controls Targeting:	
External Fraud	**Internal Fraud/Policy Issues**
Training on phishing, card security, etc.	Training on card policies and procedures
Cardholder transaction review	Usage of internal agreement
Transaction disputes, as needed	Manager review of cardholder transactions
Verification of supplier PCI compliance	Appropriate separation of duties
Card controls (e.g. limits, MCC blocks)	Card controls (e.g. limits, MCC blocks)
Auditing and program reporting	Auditing and program reporting

Source: Mercator Advisory Group

Conclusion

JPMorgan Chase is at the forefront of battling fraud in the commercial card industry. Our, four-pronged approach to managing fraud has produced strong results. Working around-the-clock to prevent fraud and improve processes is an investment in commercial card program excellence, providing our valued customers with a level of confidence that their programs will provide the full range of expected benefits. We believe that a collaborative relationship with our trusted clients, involving ongoing consultancy and sharing of best practices, help create an unparalleled level of confidence in JPMorgan Chase commercial card products.

JPMorgan Chase is at the forefront of battling fraud in the commercial card industry.