

UNDERSTANDING PAYMENTS FRAUD

In this issue

PRODUCT SPOTLIGHT

PNC provides an array of controls and protections for clients that aim to prevent card fraud, provide early warnings of fraud taking place, as well as insure against fraud that has taken place.

INDUSTRY SPOTLIGHT

Public sector organizations stand to gain a number of benefits by adopting electronic payment processes. First among them: the potential for significant cost savings.

BY THE NUMBERS

Review key statistics related to the frequency and sources of commercial card payments fraud.

QUICK TIPS

We present 10 tips companies can use to reduce their risk of payments fraud.

SPECIAL FEATURE

Making purchases with chip cards is easy when you know how.

NATIONAL ECONOMIC UPDATE

A NOTE FROM JEFF FELSER, SENIOR VICE PRESIDENT



In the current issue of *Payment Solutions News*, we take a look at the threat of payments fraud.

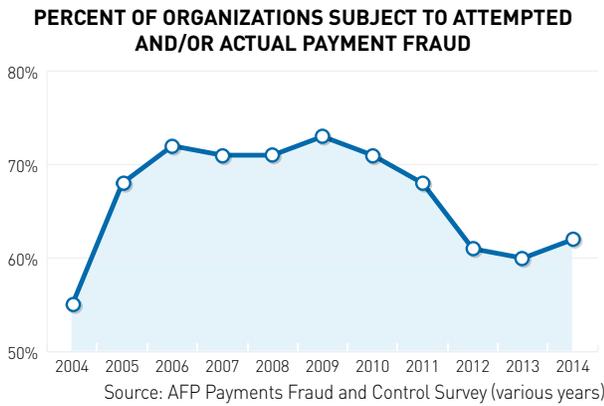
The topic has been prominent in the media in recent months due to the ongoing adoption of EMV® (chip) card technology in the U.S. and upcoming changes to the way the major card networks handle liability for fraudulent card transactions. In 2014, PNC introduced enhanced versions of our corporate cards with chip-and-PIN functionality, which we discussed in the Winter 2014 issue of *Payment Solutions News*. PNC now offers both signature and PIN-based EMV chip cards for all card programs. The introduction of EMV is significant, as it should lead to substantial declines in card fraud based on the experiences of other countries with full EMV deployment. And it could not come at a better time. The U.S. accounted for 48.2% of gross card fraud losses worldwide in 2014 (across all card types), but only 21.4% of global purchase and cash volume.¹ A recent AFP survey found that 92% of U.S. financial professionals believe that EMV cards will be effective in reducing point-of-sale fraud.²

While EMV is a powerful tool for reducing certain types of payments fraud (in particular counterfeit card fraud, which accounts for about one-third of card fraud), it will not eliminate payments fraud. Fraudsters will continue to target vulnerable parts of the payments ecosystem. Following the introduction of EMV in the UK, counterfeit card fraud fell by 56%, but card-not-present fraud rose by 79%.³ Therefore, companies and banks must remain vigilant to anticipate, identify and mitigate payments fraud threats.

This issue explores recent trends in payments fraud incidence and key areas of vulnerability, as well as identifies products and strategies that can help to protect our clients from payments fraud.

LATEST TRENDS

According to a recent survey, 62% of U.S. organizations were subjected to attempted or actual payments fraud in 2014.⁴ The following chart shows that this percentage has declined from levels seen in the mid-2000's, but reaffirms that payments fraud remains a significant threat to U.S. firms. Larger organizations (>\$1 billion in revenues) have greater exposure to payments fraud than smaller firms (65% vs. 56%).

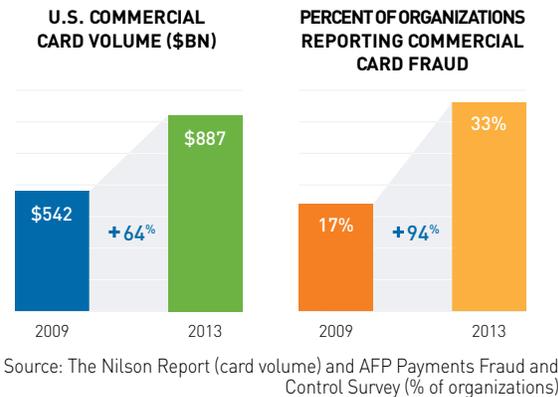


FRAUD BY PAYMENT TYPE

In terms of fraud levels by payment type, we note that changes in reported levels of fraud by payment type reflect changes in usage of that payment type. For example, **checks** have traditionally had a dominant share of business-to-business payments volume, but this share is steadily declining. Between 2010 and 2013, reported incidence of check fraud by U.S. organizations fell from 93% to 82%⁵, mirroring the decline in checks' share of business-to-business payments from 57% to 50% over the same period⁶.

It is also notable that **commercial cards** and **wire transfers** represent a growing share of both B2B payments fraud incidence and financial losses.

The percentage of organizations reporting commercial card fraud almost doubled between 2009 and 2013. To a large extent, this reflects the growing usage of commercial cards (U.S. commercial card volume grew 64% during this period). However, the U.S. has also been increasingly vulnerable to card-present fraud, as fraudsters have redirected their criminal activities away from regions that have adopted EMV.

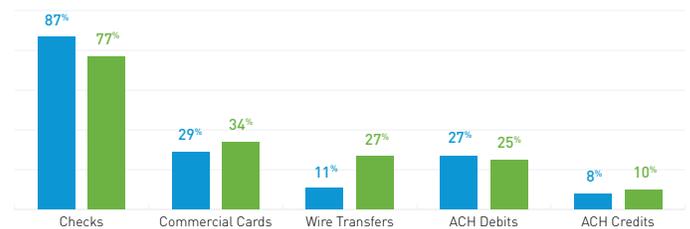


Similarly, the rise in wire transfer fraud is largely due to strong growth in transaction volume, as well as increased frequency and complexity of cyber-attacks. For example, the AFP reported that wire transfer fraud often involves email spoofing based on information gleaned in part from social media.⁷

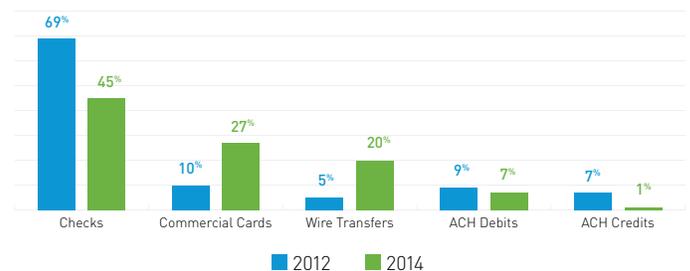
Not only have organizations reported growth in incidence of commercial card and wire transfer fraud in recent years, these payment types are also seen as responsible for an increasing share of financial losses from fraud, as fraudsters redirect their efforts away from checks and towards these payment methods.

- The percentage of organizations who reported commercial card fraud rose 5 percentage points (from 29% to 34%) between 2012 and 2014.
- During this same period, the percentage of organizations that identified commercial card as responsible for the largest dollar amount of fraud loss jumped from 10% to 27%.
- On the other hand, check fraud incidence fell from 87% to 77% between 2012 and 2014. And, the percentage of organizations identifying checks as responsible for the largest amount of fraud loss fell by 24 percentage points, from 69% to 45%.

PERCENTAGE OF ORGANIZATIONS REPORTING FRAUD BY PAYMENT TYPE



PAYMENT METHOD RESPONSIBLE FOR THE LARGEST DOLLAR AMOUNT OF FRAUD LOSS



Source: AFP Payments Fraud and Control Survey

STRATEGIES FOR REDUCING YOUR EXPOSURE TO PAYMENTS FRAUD

Companies are looking to optimize their payment processes, while also reducing their vulnerability to payments fraud. While no method of fraud protection is 100% secure, taking the following steps can help to reduce fraud and safeguard your business:

<p>Reduce check usage for B2B payments</p>	<p>Checks continue to be the main target for payments fraud , so one obvious way to reduce exposure to check fraud is to increase adoption of electronic payments. In the Spring 2015 issue of <i>Payment Solutions News</i>, we showed that U.S. businesses are moving steadily away from checks and towards electronic payments in order to reduce administrative costs, streamline reconciliation, reduce disputes with suppliers, and in general improve the bottom line.</p>
<p>Increase usage of EMV-enabled commercial cards</p>	<p>According to the Payments Security Task Force, it is expected that 63% of all credit and debit cards will be chip-enabled by the end of 2015, with 98% of cards to be converted by the end of 2017.⁸ While merchant acceptance has been slower, the Aite Group projects that 59% of U.S. merchant terminals will be able to accept EMV transactions by the end of the year.⁹ PNC incorporated chip functionality into its enhanced suite of corporate (travel and entertainment) cards in 2012. All PNC commercial card clients will be receiving chip cards automatically in the coming months.</p>
<p>Leverage the various protections offered by PNC</p>	<p>Protections provided by PNC to our commercial banking clients include:</p> <ul style="list-style-type: none"> ▪ Standard protections built into PNC products and services, such as the wide range of administrator controls on commercial cards, as well as the range of security features in our PINACLE[®] online and mobile banking portal. ▪ Dedicated fraud prevention services, such as ACH Debit Block and Positive Pay (Reverse Positive Pay, Teller Positive Pay, Point of Sale Positive Pay, ACH Positive Pay and Payee Matching). In the Product Spotlight section of the newsletter, we provide additional detail on some of the fraud prevention and mitigation tools available to PNC clients.
<p>Take practical steps to reduce exposure to payments fraud</p>	<p>Encourage card program administrators and cardholders to actively monitor their accounts as they would their personal credit cards. All cards are at risk and commercial cards with relatively high credit lines can be targets for fraudsters. In the Quick Tips section, PNC lists ten practical operational steps that our clients should take in order to minimize their exposure to payments fraud.</p>

IN THIS ISSUE

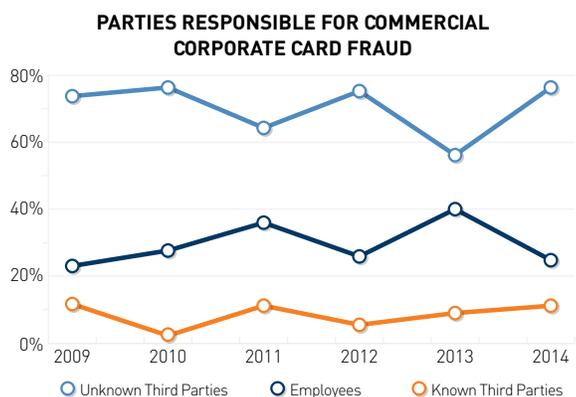
- Learn how you can protect your corporate card programs from fraud in this issue’s [Product Spotlight](#).
- Public sector and not-for-profit organizations can benefit from switching to electronic payments. See how in the [Industry Spotlight](#).
- In [Quick Tips](#), we offer ten practical steps for reducing payments fraud at your company.

Discover how PNC can deliver ideas, insights and solutions to help you achieve your objectives. Contact your Treasury Management Officer or Account Manager, or visit pnc.com/treasury.

CORPORATE CARDS: PROTECTION FROM FRAUD

In the Winter 2014 issue of *Payment Solutions News*, we discussed PNC’s launch of enhanced Visa® Corporate Cards. Between 2009 and 2014, corporate card volume at PNC rose at a 32% compound annual growth rate (CAGR)—significantly higher than 12% for American Express® and 6% for Visa/MasterCard® issuers—as our clients were availed of the many benefits provided by these travel-and-entertainment (T&E) cards.

When companies deploy corporate cards, they must ensure that there are safeguards in place to protect against both external and internal fraud. According to the 2015 AFP Payments Fraud and Control Survey, unknown external parties were responsible for 77% of corporate/commercial card fraud, followed by employees (25%) and third-parties/outsourcers (16%).¹⁰ *Note that percentages add to more than 100%, as a fraud attempt could be attributed to multiple parties.*



Fraud protection for our commercial payments clients has consistently been a critical area of focus at PNC. Our efforts in this regard have been recognized by the payments industry, most recently in Visa’s 2014 Service Quality Awards. PNC received the Highest Authorization Approval Rate award for international transactions, as well as the Highest Non-Fraud Chargeback Effectiveness award.

DID YOU KNOW?

PNC works hard to reduce fraudulent transactions for companies and employees. Over the last quarter, PNC prevented \$700,000 worth of fraudulent activity that would have occurred on over 1,400 accounts. These fraudulent attempts occurred on nearly 5,000 transactions across the more than 7.5 million transactions that PNC Commercial Card services processed over that time period.

Less than half a percent of our transactions are false positive, meaning over 99.5% of transactions that PNC blocks due to fraud are actually fraudulent in nature. PNC continues to invest in ways to minimize fraud while ensuring authorized company cardholders do not experience declines at the point of sale.

PNC provides an array of controls and protections for clients that aim to prevent card fraud, provide early warnings of fraud taking place, as well as insure against fraud that has taken place.

In addition, we work closely with clients to help ensure that these solutions are being effectively deployed. The table on the following page provides insight into PNC’s fraud protection measures.

CORPORATE CARDS: PROTECTION FROM FRAUD

	PREVENTION			DETERMINATION			MITIGATION		
	Card Controls			Monitoring and Alerts			Insurance		
Protection	Merchant category code (MCC) restrictions	Spending limits	Other restrictions	Visa Advanced Authorization	Compromised Account Management Systems (CAMS)	Text alerts	Insurance for employee fraud or misuse		
Additional Detail	Limits cardholder spending to specific merchant types related to their business activities	Limits on individual purchase amounts or number of card transactions per day/month	Restrictions on cash withdrawals or international usage	24x7 fraud monitoring that uses risk detection technologies to evaluate authorizations and alert clients to potential fraud in real time	Visa fraud alert system that reports stolen/ recovered or compromised cards to all issuers	Cardholders receive text messages when suspicious activity is detected on their cards	Visa Liability Waiver Program provided at no additional cost	Coverage of up to \$100,000 per card under the Program	Coverage begins 75 days prior to termination notice and extends to 14 days after termination notice
What Client Needs To Do	Controls are set by the program administrator, and can be customized at the cardholder, department or organization level.			Cardholder elects to receive alerts, Cardholder verifies the suspicious activity or files a notification of fraud activity			Client must contact PNC to request that liability for fraudulent charges be waived in accordance with the Visa Commercial and Business Card Liability Waiver Program		

COMING SOON

PNC is readying the launch of our newest tool in the fight against payments fraud, Visa IntelliLink® Compliance Auditor. Designed for card program administrators and auditors, Visa IntelliLink Compliance Auditor monitors transactions and identifies questionable purchases.

By accessing detailed transaction documentation, the tool can help to uncover fraud and card misuse. Talk to your PNC Treasury Management Officer for more information.

Meet with your Treasury Management Officer or Account Manager to learn more about how to protect your company from the threat of payments fraud.

ELECTRONIC PAYMENTS IN THE PUBLIC SECTOR

The U.S. public/not-for-profit sector is comprised of a diverse array of organizations, including government agencies, authorities, educational institutions and general not-for-profit organizations.

While each sector has different areas of focus, structures, cultures and business practices, public/not-for-profit organizations share characteristics and needs that suggest that they could benefit greatly from adopting electronic payments.

 <p>GOVERNMENT</p>	<ul style="list-style-type: none"> States Counties Authorities Municipalities School Districts
 <p>EDUCATION</p>	<ul style="list-style-type: none"> Universities Colleges Community Colleges Public & Private Institutions Charter Schools
 <p>NOT-FOR-PROFIT</p>	<ul style="list-style-type: none"> Cultural Philanthropic Research Advocacy Services

ELECTRONIC PAYMENTS CAN LEAD TO SIGNIFICANT COST SAVINGS

- The Smart Cities Council reported that the **City of Toronto** saved \$2 million per year from switching from cash and checks to debit cards for social benefits payments.¹¹
- An NAPCP study reported that city governments saved \$35.50 to \$164 per transaction in switching from purchase orders to purchasing cards. The **Washington State Department of Transportation** generated estimated annual savings of \$4.7 million from using purchasing cards and ghost accounts rather than traditional purchase orders for almost half of its transactions.¹²

Interestingly, the same characteristics that make public/not-for-profit organizations excellent candidates likely to benefit from electronic payments adoption can also prevent these organizations from fully capturing the efficiencies from these payments systems.

The following table identifies common public/not-for-profit characteristics and shows areas where electronic payments adoption can be beneficial. Conversely, the table also points out several potential issues that could arise due to the often unique structural and operational set ups of these organizations.

Public/not-for-profits' structural and cultural characteristics...	...create a significant opportunity for electronic payments adoption...	...but complicate the implementation of an electronic payments system
Desire for Transparency and Accountability	Electronic payments are more transparent than paper-based systems, with more streamlined reporting and more accurate monitoring.	The same need for transparency can complicate the decision-making process and rollout.
Large and Diverse Payments Volume	Financial controllers and administrators tend to have significant interest in solutions and systems that can streamline receivables and payables and reduce payments complexity.	Legacy systems add to the sheer complexity in switching to a new payment system and can seem overwhelming.
Budget Constraints and Structures	The ongoing pressure to remain within annual budget targets creates interest in products and tools that can increase efficiency.	Budget planning tends to be done on an annual basis, which can hinder the ability to make significant investments in new payments systems that pay off in the longer term.
Administrative Focus	Switching to electronic payments has been proven in both public and private sectors to dramatically reduce administrative costs, e.g., by streamlining the reconciliation process.	However, hierarchical and complex treasury structures can complicate decision-making and implementation. And the administrative burden can persist beyond implementation.
Employee Practices	<p>Public sector employees tend to have strong participation in training programs, which facilitates the transition to electronic payments.</p> <ul style="list-style-type: none"> A 2014 study by the NAPCP and Mercator Advisory Group found that 86% of public sector organizations mandate cardholder training prior to issuance, compared to only 53% of private sector organizations. And 61% of public bodies mandate follow-up training, again significantly higher than private firms (24%). 	<p>Employees tend to take a measured approach when switching from tried-and-trusted processes and practices.</p> <ul style="list-style-type: none"> An NAPCP/Mercator study found that 31% of public organizations manually audit all of their purchasing card/one card transactions, compared to 15% of private sector organizations.

For public/not-for-profit organizations to fully capture the cost savings and other benefits from transitioning to electronic payments, they need to partner with a financial provider that understands these structural and operational hurdles, and that has the experience and expertise of operating in this unique environment.

PNC PUBLIC FINANCE GROUP

PNC established the Public Finance Group to provide products and services to help our public and not-for-profit clients maximize cash flow, raise capital, mitigate risk and manage assets. Our treasury management services for public

sector and not-for-profit organizations include industry-leading and comprehensive payment and collections services. We remain at the forefront of electronic payments development, including an award-winning suite of card services, nationally recognized collections services, and sophisticated fraud mitigation techniques to help centralize, control and protect your treasury system.

PNC supports these products and services with specialized teams who provide quick and effective implementation, as well as client care teams who work closely with our public and non-for-profit clients to ensure ongoing success and satisfaction.

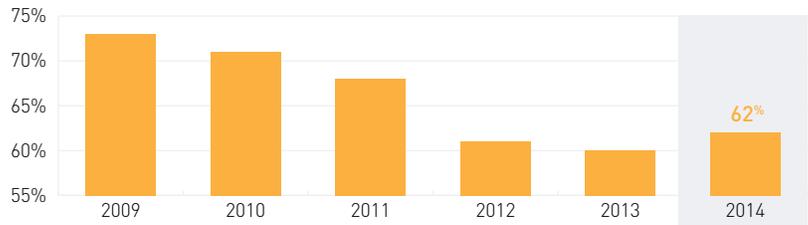
The PNC Public Finance Group delivers this combination of product breadth and high-touch client support to nearly 500 state, county and municipal government entities and authorities, more than 150 institutions of higher education, and more than 600 school districts and not-for-profit organizations.

For more information about the PNC Public Finance Group, contact PNC today.

PAYMENTS FRAUD IN COMMERCIAL CARDS

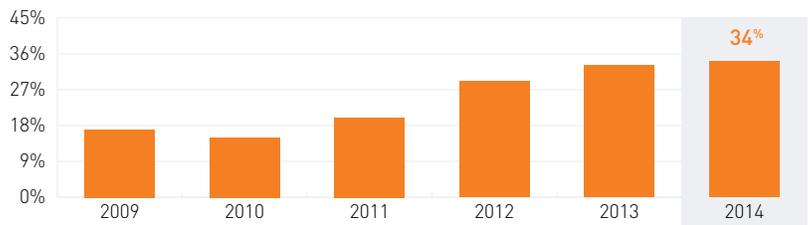
Among the **62%** of organizations who reported attempted or actual payment fraud in 2014...

PAYMENT FRAUD INCIDENCE



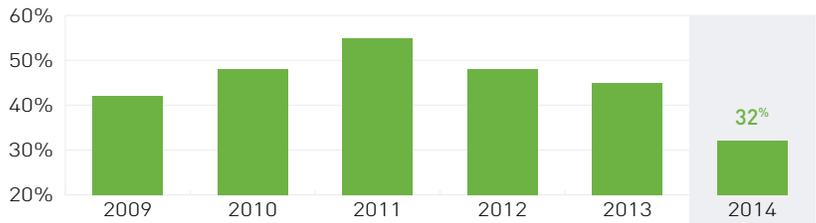
...**34%** reported commercial card fraud.

COMMERCIAL CARD FRAUD



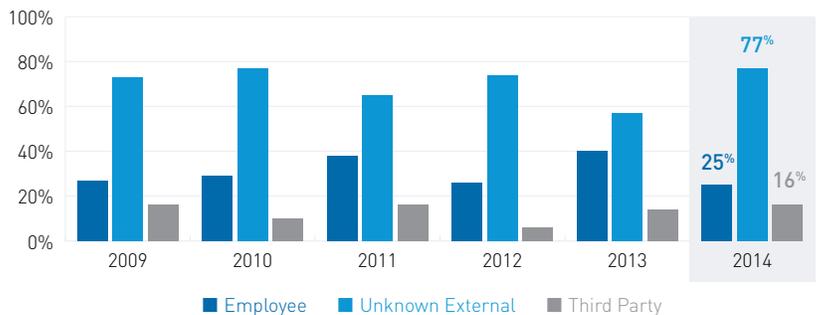
Of the organizations reporting commercial card fraud, **32%** reported fraud on their own corporate cards.

FRAUD ON OWN COMMERCIAL CARDS



For **77%** of organizations who reported fraud on their own commercial cards, the fraud was initiated by an unknown external party. **25%** of companies reported own commercial card fraud by company employees, and **16%** by known third parties.

SOURCES OF FRAUD ON OWN COMMERCIAL CARDS



Source: 2015 AFP Payments Fraud and Control Survey

10 PRACTICAL STEPS TO REDUCE FRAUD RISK

Here are ten actions you can take to reduce the risk of payments fraud at your company:

- 1 Review your company's payment controls and procedures; identify key deficiencies; implement quick fixes in critical areas.
- 2 Analyze spending patterns for your organization's key spending units; develop a plan and benchmarks to transition to electronic payments; recruit suppliers to accept electronic payments.
- 3 Perform daily reconciliations of all transaction activity.
- 4 Separate administrative, approval, auditing and reconciliation duties.
- 5 Establish processes for administrators to act immediately on suspicious payment activity.
- 6 Adopt stronger forms of authentication to access company networks or bank services and employ them consistently across channels (e.g., web, mobile, call center).
- 7 Analyze spending patterns by traveling employees and key executives, and actively monitor for attempted activity in unusual geographies.
- 8 Create and communicate card usage policy; apply card usage controls (on total spending, merchant categories, etc.).
- 9 Educate all employees on various types of cyber fraud, and how to protect against such attacks.
- 10 Maintain an ongoing dialog with your PNC account team to take advantage of the bank's wide array of payments fraud protection services.

MAKING PURCHASES WITH CHIP CARDS



The way that you use a credit or debit card to make a purchase is changing. With the U.S. adopting the EMV payment standard (see the Spring 2015 issue of *Payment Solutions News* for full details), merchants and credit card issuers are migrating to chip-based card transactions.

These transactions require:



Chip-Enabled Terminals

New credit card terminals are equipped to read microchip information from cards.



Chip Cards

These credit and debit cards have chips embedded into the plastic.

STEP

1



Insert your card into the slot in the front of the terminal.

Be sure the chip is facing up.

Leave the card in the reader.

STEP

2



With your card in the reader, follow the prompts.

- For chip-and-PIN cards, you may be prompted to enter your PIN.
- For chip-and-signature cards, you may be asked to provide a signature.

STEP

3



Remove your card when prompted and take your receipt. Your transaction is complete.

¹ The Nilson Report, #1068, July 2015

² 2015 AFP Payments Fraud and Control Survey, Association for Financial Professionals

³ "As Big Banks Prep for EMV, Fraud Relief Remains Far Off," Bank Technology News, March 18, 2015

⁴ 2015 AFP Payments Fraud and Control Survey, Association for Financial Professionals.

⁵ AFP Payments Fraud and Control Survey, 2010 and 2013

⁶ 2013 AFP Electronic Payments Survey

⁷ "Wire Transfer Fraud Picks Up," Treasury & Risk, May 13, 2015

⁸ "Issuers Forecast U.S. Shift to Chip Cards To Be Nearly Complete by 2017," MasterCard News Release, May 4, 2015

⁹ "More Than Half of U.S. POS Terminals to Be EMV Chip-Enabled by Year-End 2015," Aite Group News Release, February 12, 2015

¹⁰ "As City Governments Eye New Tech, Payments Play a Vital Part," Payments Source, March 11, 2014

¹¹ "Cost Savings: Purchasing Cards vs. Traditional Purchase Orders in the Government Sector," NAPCP Benchmark Report, February 2015

¹² "Sectors Can Learn Something from Each Other: A Bright Spot Shared by Both Sectors," TransAct! Newsletter, January 30, 2015

This PNC Payments Solution News was prepared for general information purposes and is not intended as legal, tax or accounting advice or as recommendations to engage in any specific transaction, and does not purport to be comprehensive. Under no circumstances should any information contained in this newsletter be used or considered as an offer or commitment, or a solicitation of an offer or commitment, to participate in any particular transaction or strategy. Any reliance upon any such information is solely and exclusively at your own risk. Please consult your own counsel, accountant or other advisor regarding your specific situation. Neither PNC Bank nor any other subsidiary of The PNC Financial Services Group, Inc. will be responsible for any consequences of reliance upon any opinion or statement contained here, or any omission.

PNC, PINACLE and ActivePay are registered marks of The PNC Financial Services Group, Inc. ("PNC"). All other trademarks are the property of their respective owners.

Bank deposit, treasury management and lending products and services are provided by PNC Bank, National Association, a wholly owned subsidiary of PNC and Member FDIC.

Lending and leasing products and services, including card services and merchant services, as well as certain other banking products and services, may require credit approval.

The American Express trademarks, logos and service marks ("Marks") are the property of American Express and other parties.

MasterCard is a registered trademarks of MasterCard International Incorporated.

Visa & Visa IntelliLink are registered trademarks of Visa International Service Association in the United States and used under license.

EMV is a registered trademark in the U.S. and other countries, and is an unregistered trademark in other countries, owned by EMVCo.

©2015 The PNC Financial Services Group, Inc. All rights reserved.