2012 PAYMENTS FRAUD SURVEY

Summary of Results, April 2012

Introduction

In April 2012, the Fifth District's Payments Studies Group conducted research on payments-related fraud experienced by regional financial institutions and businesses.[1,2] Constituents in the District were asked to respond to an online survey about their experiences with payments fraud and the methods they used to minimize fraud risk. In addition, the survey audience was expanded with the help of the Fifth District Business and Consumer Payments Advisory Councils' (BACPAC) participation and by mass digital media communications (tweets) informing the "followers" of the FRB Richmond of the ongoing survey.[3] Payments covered in the survey included transactions for 2011 involving cash, check, debit and credit cards, and automated clearinghouse (ACH) and wire transfers.[4]

Respondent Information

The survey was sent to approximately 880 Fifth District organizations of which 95 participated for a response rate of 11 percent.[5] The share of respondents by state and organization is as follows:

Table 1: Share of Responses by State and Organization (N=95)

	Financial Institutions		Businesses	Total (%)	Total (#)
	Banks	Thrifts			
Maryland	17% (16)	1% (1)	3% (3)	21%	20
Virginia	36% (34)	1% (1)	2% (2)	39%	37
West Virginia	16% (15)	0% (0)	0% (0)	16%	15
North Carolina	9% (9)	0% (0)	1% (1)	10%	10
South Carolina	12% (11)	2% (2)	0% (0)	14%	13
TOTAL	**90% (85)**	**4% (4)**	**6% (6)**	**100%**	**95**

The concentration of financial institution respondents with under $50 million appears consistent with the association and influence of the Independent Community Bankers of America (ICBA) (Table 2). More than half of the banks that responded to the survey are members of the ICBA. No responses were received from any financial institution with more than $5 billion in annual revenue.

Table 2: Respondents by Annual Revenue (N=95)

	Financial Institutions		Businesses	Total (%)	Total (#)
	Banks	Thrifts			
Under $50 million	57% (54)	3% (3)	1% (1)	61%	58
$50–$99 million	3% (3)	0% (0)	1% (1)	4%	4
$100–$249.9 million	7% (7)	0% (0)	2% (2)	10%	9
$250–$499.9 million	8% (8)	1% (1)	0% (0)	10%	9
$500–$999.9 million	4% (4)	0% (0)	0% (0)	4%	4
$1–$4.9 billion	2% (2)	0% (0)	0% (0)	2%	2
$5–$9.9 billion	0% (0)	0% (0)	1% (1)	1%	1
Over $10 billion	0% (0)	0% (0)	1% (1)	1%	1
Don't know or not applicable	7% (7)	0% (0)	0% (0)	7%	7

Summary of Survey Results by Questions

This section summarizes survey responses by question. Where differences are relevant, responses of the financial institutions are reported separately from all others.

Payment Types Used by Non-Financial Institution Respondents

Non-financial institution respondents were asked about the typical payment types accepted and used for disbursements. Charts 1 and 2 show the responses. (Right)

Payment Products Offered by Financial Institution Respondents

The table below shows the types of customers typically targeted by the payment products offered by financial institution (FI) respondents. The customer base varies by the type of financial institution, with 86 percent of banks offering these products to both consumers and businesses, while 25 percent of thrifts have products geared specifically for the consumer.

Table 3: Type of Customers to Whom Financial Institutions Offer Payments Products and Services

Target Customers	Banks (N=85)	Thrifts (N=4)
Both Consumers and Businesses or Commercial Clients	86%	75%
Primarily Consumers	7%	25%
Primarily Business or Commercial Clients	7%	0%

Chart 1: Payment Types Accepted by % of Non-Financial Institution Respondents (N=6)

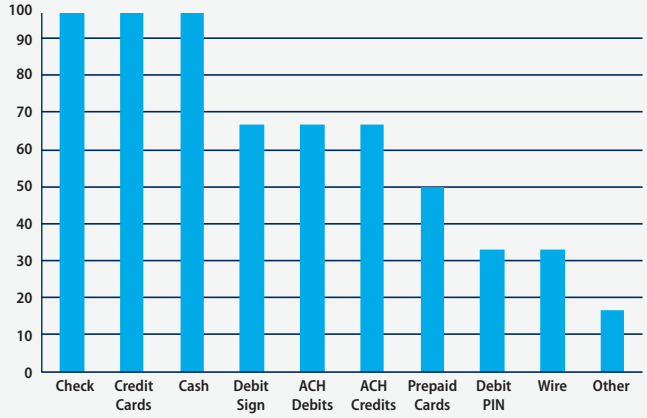
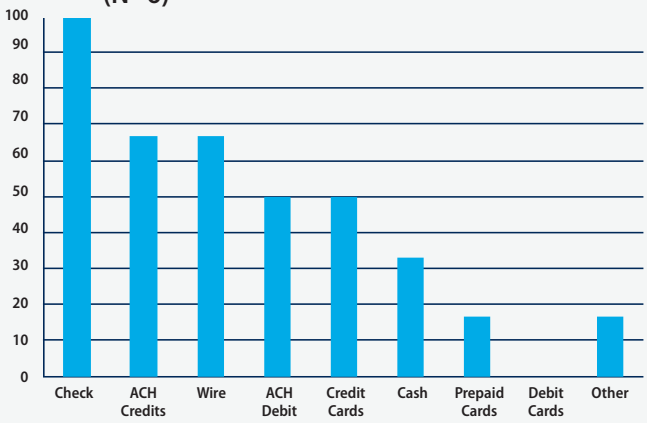


Chart 2: Payment Types Used for Disbursements by % of Non-Financial Institution Respondents (N=6)



Nearly all financial institutions offer wire transfer, PIN debit, bill payments and check products as shown in Chart 3. Over 80 percent offer half of the 12 payment products. A higher percentage of thrifts offer mobile and credit cards, which may reflect their focus on consumers.

Payments Fraud Attempts and Financial Losses

All Fifth District institutions reported some form of fraud attempts. The payment type with the highest number of fraud attempts for Fifth District organizations was signature debit, with 71 percent (see Chart 4).[6] Check, PIN debit cards and credit cards rounded out the top four. While this pattern was the same for the financial institutions, businesses experienced the highest number of fraud attempts on checks and credit cards. Despite the rapid growth in the general purpose reloadable card segment, no significant fraud attempts with prepaid cards were reported by any of the Fifth District institutions included in the survey.

Respondents were asked which payment types experienced the highest dollar losses (Chart 5). Seventy-three percent of FIs identified signature debit cards as having the highest financial losses, followed by checks and PIN-based debit cards. In contrast, for the non-FI Fifth District organizations, all reported credit cards as having the highest dollar losses, with cash (60 percent) and checks (40 percent) following. Overall, highest dollar losses were experienced with signature debit cards, checks and PIN-based debit cards.

For each payment type, respondents were asked whether fraud prevention costs or actual fraud losses were a greater expense for their organization. For a majority of financial institutions (Chart 6), debit card products had higher fraud losses than prevention costs. Fifty-seven percent of the FI respondents reported actual losses on signature debit cards greater than prevention costs, while 53 percent experienced higher actual losses on PIN-based debit than the prevention costs. This suggests that some financial institutions could gain from increased investments in fraud deterrence, as their losses currently exceed prevention outlays.

For all non-financial institution respondents, prevention costs for checks and ACH exceeded actual fraud losses (see Chart 7). Respondents were evenly split on their costs versus losses on credit cards: Half reported that actual losses exceeded prevention costs while the other half reported the reverse.

Chart 3: Payment Products and Services Offered by % of Financial Institution Respondents

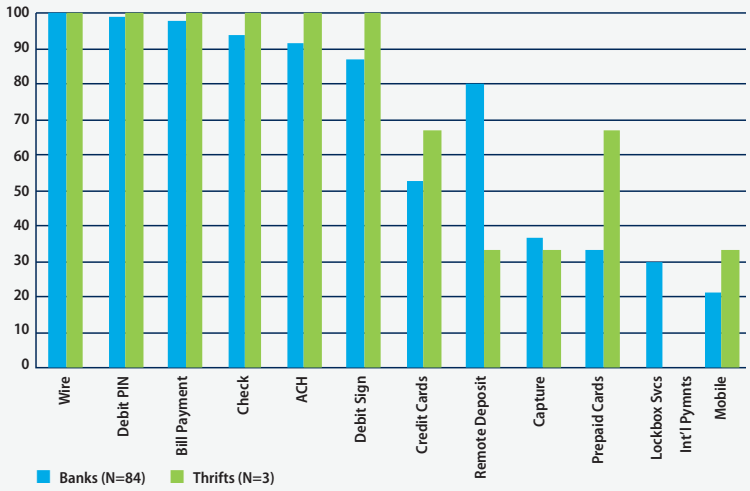


Chart 4: Payment Types With Highest Number of Fraud Attempts by % of Respondents

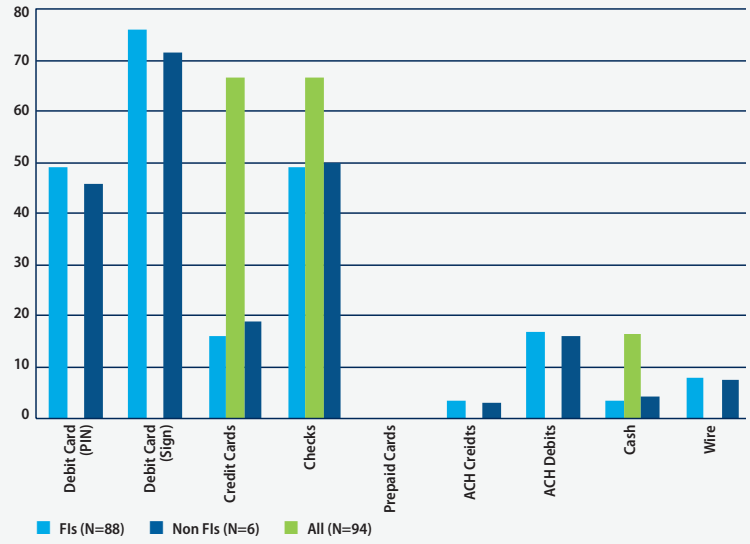
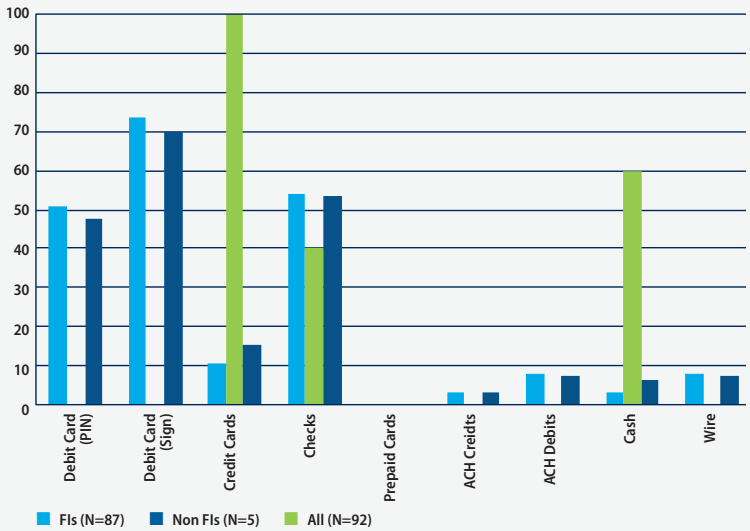


Chart 5: Payment Types With the Highest Dollar Losses by % of Respondents



For the overwhelming majority of respondents (92 percent), losses as a percentage of total annual company revenue were at or below 0.5 percent (Table 4). For all of the non-FIs, losses were less than 0.3 percent of total revenue. This would suggest that losses in general are relatively modest and well controlled. It is also expected that financial institutions would have greater exposure to financial fraud than their counterparts in business given their greater points of contact with the public. This greater consumer access would also suggest that perpetrators of fraud go after the more convenient and accessible targets of opportunity.

For the majority of Fifth District respondents (52 percent) the incidence of fraud between 2011 and 2010 had increased. This increase in fraud mainly affected the financial institutions, as no increases in losses were incurred by the non-financial institutions (Table 5). This is consistent with observations from the Association for Financial Professionals' (AFP) 2012 Payments Fraud and Control Survey. In the report, it was observed that losses decreased for most organizations in 2011. The AFP survey has a broader industrial coverage than the Federal Reserve Bank survey, with banking or financial services accounting for just 7 percent of the institutions.

Financial institution respondents, which had indicated increases in losses, also gave an estimate of that increase, with approximately half reporting an increase in the 1 to 5 percent range (Chart 8). A significant proportion (21 percent) was unsure of the rate, while 18 percent felt the increase in dollar losses exceeded 10 percent.

Respondents were asked to identify the top payment types underlying the increases in fraud

Chart 6: Fraud Prevention Costs vs. Actual Fraud Losses by % of Financial Institution Respondents (N=69)

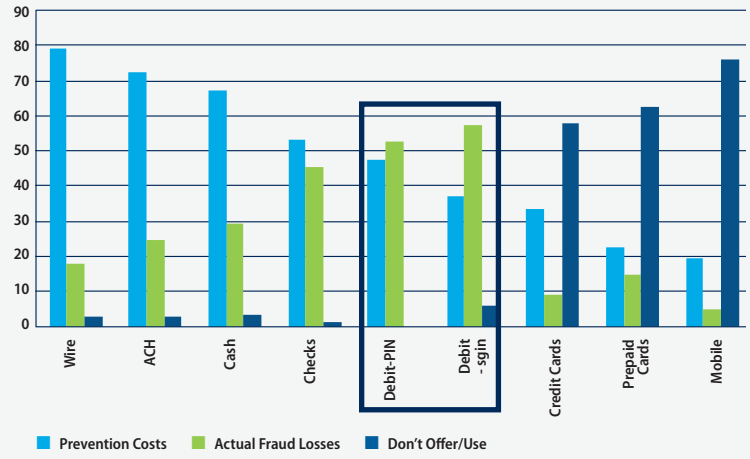


Chart 7: Fraud Prevention Costs vs. Actual Fraud Losses by % of Non-Financial Institution Respondents (N=4)

Table 4: Loss Range as a % of Revenue (N=88)

	0%≤ - <0.3%	0.3% - 0.5%	0.6% - 1%	1.1% -5%	Over 5%
FIs (N=83)	77%	15%	5%	4%	0%
Non-FIs (N=5)	100%	0%	0%	0%	0%
All Respondents	78%	14%	4%	3%	0%

Table 5: Change in Losses in Last 12 Months (N=92)

	FIs (N=87)	Non-FIs (N=5)	All (N=92)
Increased	55%	0%	52%
Decreased	15%	20%	15%
Stayed the Same	30%	80%	33%

losses they experienced (please see Table 6). The top three were signature debit cards, PIN debit cards and checks. Signature debit cards were nearly twice as likely to be chosen as the top contributor to increases in fraud losses than the next highest candidate — PIN debit cards. Previously, signature debit cards were also highlighted as experiencing the highest number of fraud attempts and highest dollar losses among payment types for Fifth District survey takers.

Table 6: Payment Type Underlying Increases in Fraud Losses by % of Respondents

	All (N=48)
Debit Cards - Signature	77%
Debit Cards – PIN	42%
Checks	31%
Wire	8%
ACH Debits	6%
ACH Credits	4%
Credit Cards	2%
Cash	2%

Decreases in fraud losses in the last year were reported by 15 percent of survey respondents. Approximately 43 percent of these respondents believed the decline in losses was more than 10 percent (Chart 9). All the non-financial institutions estimated the decline in losses at more than 10 percent.

These respondents were asked to identify key factors that contributed to the decline in the rate of fraud losses in the last 12 months. The four key factors that were cited most by the respondents were: staff training and education, enhanced fraud monitoring, enhanced internal controls, and the use of ACH positive pay.

Chart 8: Increase in Loss Rate by % of Financial Institution Respondents (N=48)

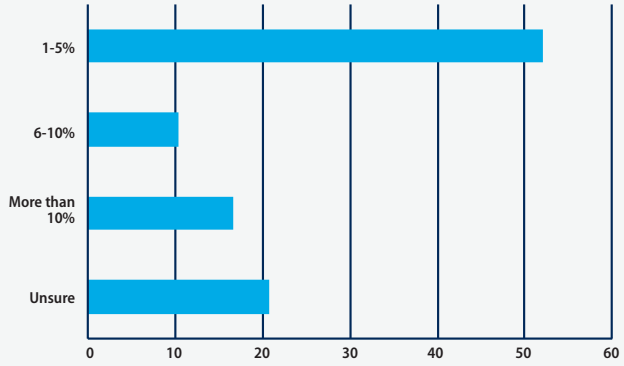


Chart 9: Decrease in Loss Rate by % of Respondents (N=14)

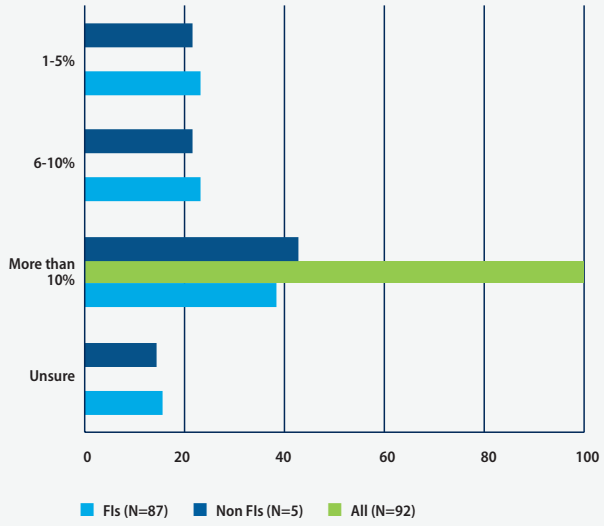


Table 7: Key Factors for Decreases in Fraud Losses by % of Respondents

	FI (N=9)	Businesses (N=1)	All (N=10)
Staff Training & Education	78%	100%	80%
Enhanced Fraud Monitoring	67%	0%	60%
Enhanced Internal Controls	56%	0%	50%
Use of ACH Positive Pay	56%	0%	50%
Enhanced Validation of Customer	22%	0%	20%
Other	11%	0%	10%

Perpetrators Involved in Successful Payments Fraud

Most respondents reported that external entities were most often responsible for successful payments fraud, with 52 percent attributing all fraud attempts to external sources. Only 3 percent of all respondents attributed all successful payments fraud to internal parties alone. Approximately 38 percent of respondents blamed a mix of perpetrators, while 7 percent could not determine the identity of the perpetrators.

Table 8: Perpetrators Involved in Successful Payments Fraud by % of Respondents (N=90)

Perpetrators	1-25%	26–50%	51–75%	76–99%	100%
Internal Only	7%	0%	1%	2%	3%
Internal With External	2%	4%	0%	0%	2%
External Only	1%	2%	2%	13%	52%
Undetermined	9%	2%	0%	0%	7%

Most Common Fraud Schemes

Each respondent was asked to identify the three main fraud schemes it experiences involving payments the organization received from or on behalf of customers and against the organization's own accounts. Chart 10 lists the top fraud schemes for payments accepted by or on behalf of customers from the financial institutions. The most prevalent schemes reported by financial institutions were counterfeit or stolen cards used at the point-of-sale (POS) or with online sales and counterfeit checks at the POS or over-the-counter (OTC). The most prevalent schemes reported by all other organizations (Chart 11) were counterfeit checks and counterfeit or stolen cards used online.

Chart 10: Top Current Fraud Schemes Involving Payments Accepted by or on Behalf of Customers by % of Financial Institution Respondents

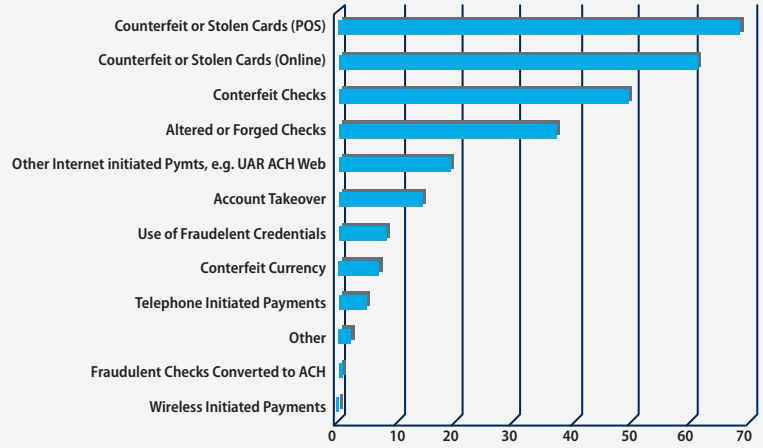


Chart 11: Top Current Fraud Schemes Involving Payments Accepted by Non-FI Respondents

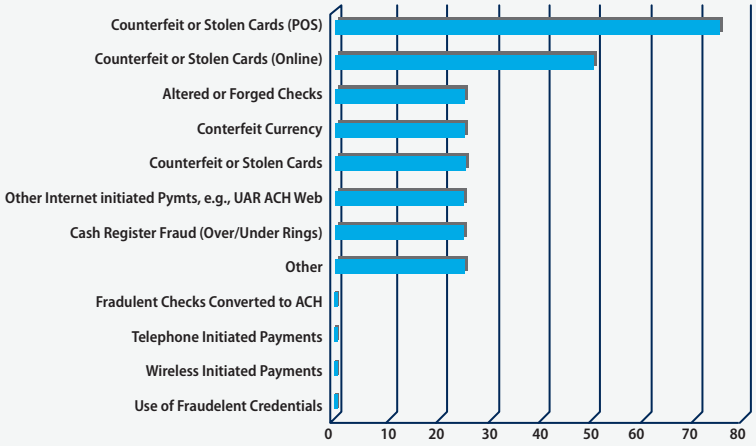


Chart 12 lists the fraud schemes reported by respondents that targeted the organization's own accounts. The most prevalent involved counterfeit checks, altered or forged checks, and fraudulent or unauthorized card transactions. Non-financial institutions were subject to a significant number of fraudulent card transactions as well as counterfeit checks.

Table 8 lists the top three sources of information used in the major fraud schemes. Two-thirds of all respondents identified "sensitive" information obtained from a lost or stolen card, check or other physical document or device while in the consumer's control (66 percent), and 43 percent identified cyberattacks, such as phishing. Information sources identified by financial institution respondents versus other organizations differed. For example, half of non-FI respondents reported that their organization's information was obtained from a legitimate check issued by the organization or by data breaches due to cyberattacks.

Chart 12: Top Fraud Schemes That Targeted Respondents' Own Accounts

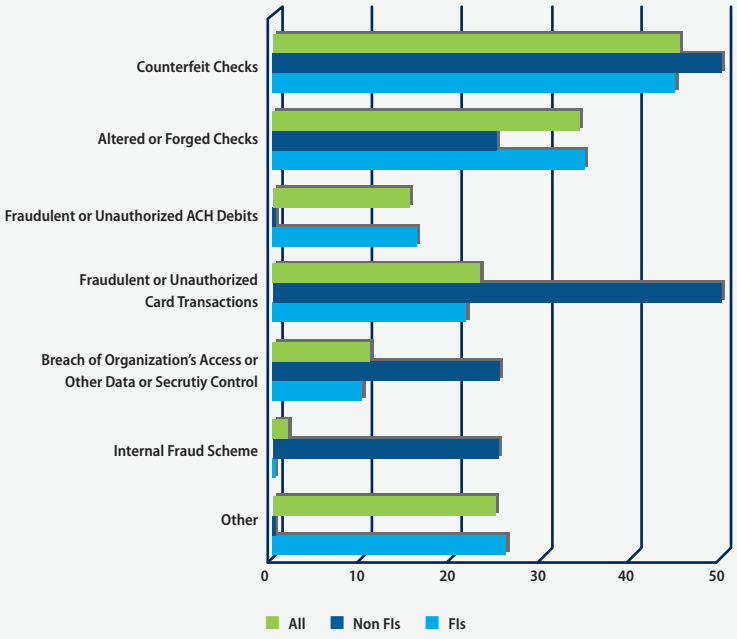


Table 8: Top Three Sources of Sensitive Information Used in Top Fraud Schemes

	FIs (N=84)	Non-FIs (N=4)	All (N=88)
Sensitive Information Obtained From Lost or Stolen Card, Check or Other Physical Device or Document While in Consumer's Control	69%	0%	66%
Phishing, Spoofing, Pharming or Other Cyberattacks Used to Obtain Sensitive Customer Information	44%	25%	43%
Skimming of Card Magnetic Stripe Information	35%	0%	33%
Organization's Information Obtained From a Legitimate Check	23%	50%	24%
Data Breaches Due to Cyberattacks Against the Organization's Information	21%	50%	23%
Information About Customer Obtained by Family or Friend	21%	25%	22%
Data Breaches Due to Lost or Stolen Physical Documentation or PC/ Electronic Device While in Control of the Organization	0%	25%	1%
Employee With Legitimate Access to Organization or Customer Information	0%	25%	1%

Payment Fraud Mitigation Method Used

Respondents were asked about their use of and the effectiveness of various types of fraud mitigation methods and tools. Questions were asked in three areas including: i) internal controls and procedures; ii) customer authentication, transaction screening and risk management; and iii) risk mitigation services offered by financial institutions.

Internal controls and procedures are the fraud mitigation methods of choice for Fifth District respondents. Over 70 percent of the institutions use 13 of the 15 controls and procedures listed in Chart 13. The top three controls used by more than 96 percent of respondents were periodic internal/external audits, authentication and authorization controls to payment processing, and addressing exception items in a timely manner.

Though use rates for customer authentication, transaction screening and risk management are lower than for internal controls and procedures, these rates are still high, with 60 percent of respondents using 10 of the 14 methods identified (Chart 14). The top two methods — providing staff education and training on fraud risk mitigation and PIN authentication — were used by more than 90 percent of respondents. Biometrics authentication, often viewed as the authentication method of the future, remains barely used at less than 10 percent, with minimal plans for uptake by 2014.

The top three risk mitigation services offered by the financial institution respondents were multifactor authentication controls to initiate payments, online information services and account alert services (see Chart 15). There is a sharp decline in the percentage of respondents offering the latter service relative to the top two, but it appears that institutions plan to increase that offering in the near future. This is likely related to the relatively small size of the respondent banks (54 percent below $50 million in annual revenue).

Barriers to Reduce Payments Fraud

Respondents reported the existence of various impediments to creating or strengthening fraud mitigation controls at their organizations (Table 9). The top three reasons were identified as: lack of staff resources, consumer data privacy issues or concerns and lack of a compelling business case. Non-financial service organizations also cited the high cost of implementing commercially available fraud detection tools or methods.

Chart 13: Use & Effectiveness of Internal Controls and Procedures by % of Respondents

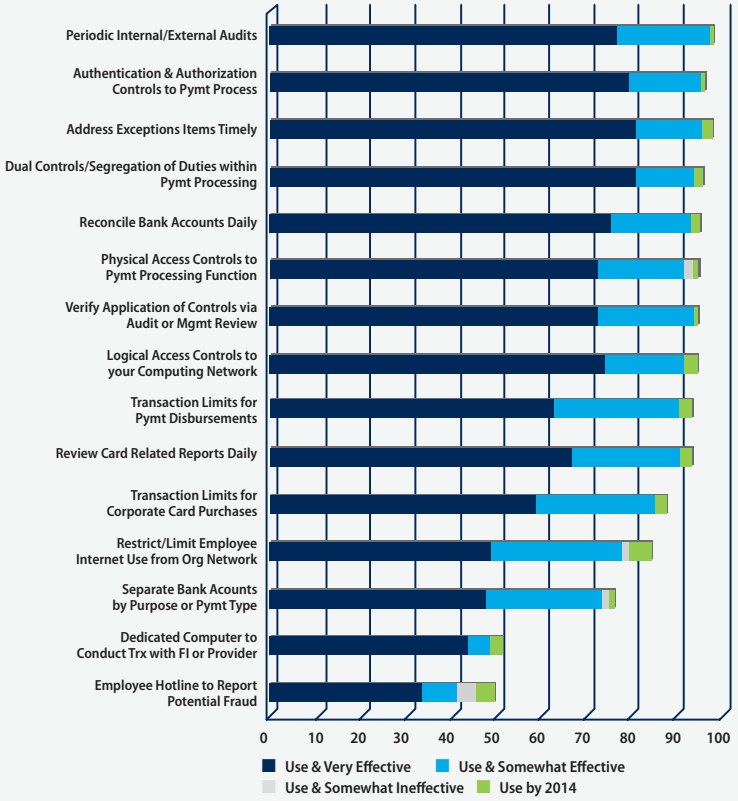


Chart 14: Use & Effectiveness of Authentication, Transaction Screening & Risk Management by % of Respondents

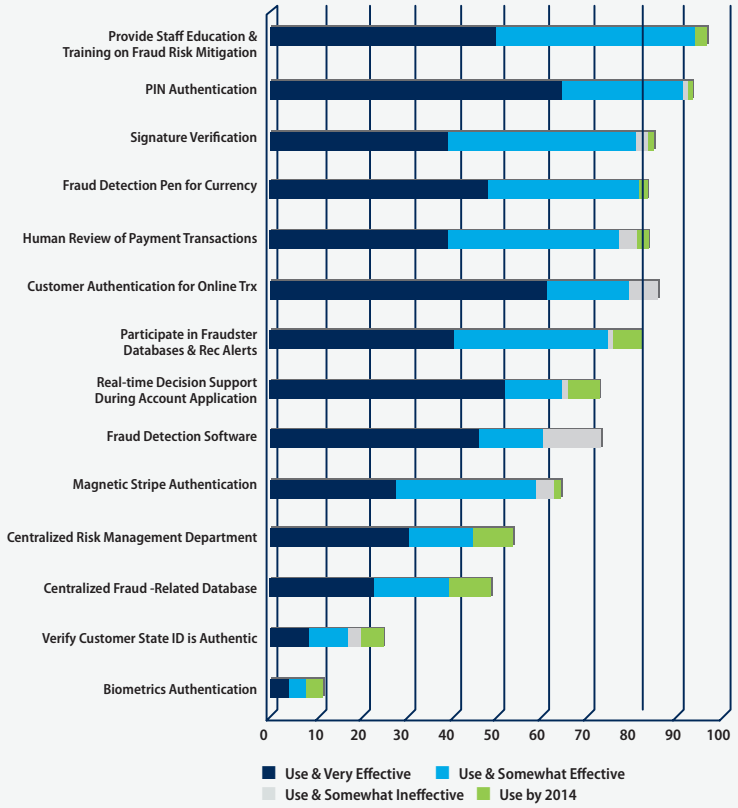
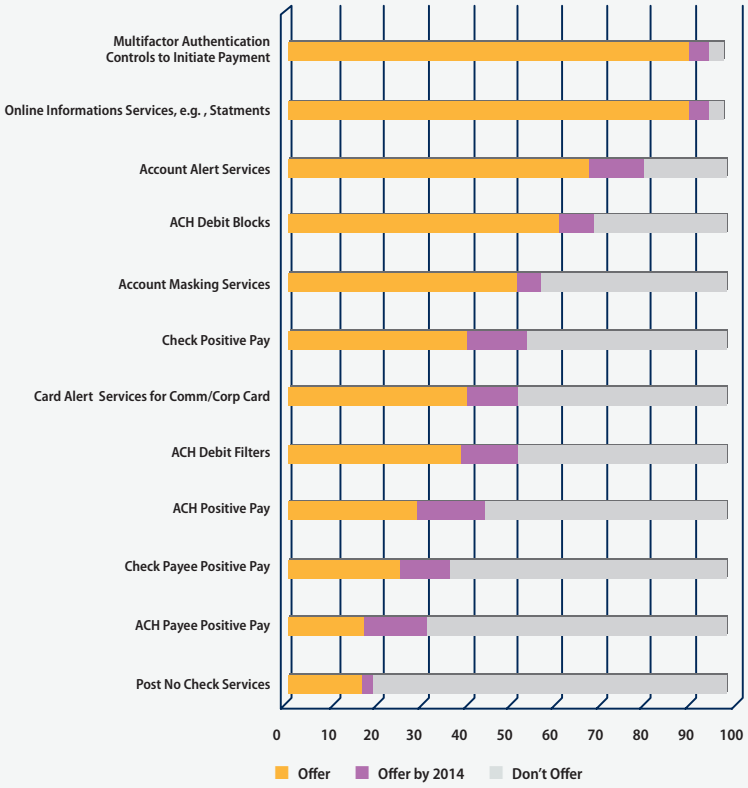


Table 9: Barriers to Reduce Payments Fraud by % of Respondents

	FI (N=67)	Non-FI (N=4)	All (N=71)
Lack of Staff Resources	63%	100%	65%
Consumer Data Privacy Issues/Concerns	39%	25%	38%
Lack of Compelling Business Case	37%	0%	35%
Cost of Implementing In-house Fraud Detection Tool/Method	33%	25%	32%
Cost of Implementing External Fraud Detection Tool/Method	30%	75%	32%
Corporate Reluctance to Share Info due to Competition	13%	0%	13%
Unable to Combine Payment Info for Review due to Scattered Operations	10%	0%	10%
Other	5%	0%	4%

Chart 15: Risk Mitigation Services Offered by % Financial Institution Respondents



Opportunities to Reduce Payments Fraud

Respondents reported on opportunities to reduce fraud in three areas: i) organization actions, ii) new authentication methods and iii) legal and regulatory changes.

With respect to an organization's action on new and improved methods, most needed to reduce payments fraud, and nearly 70 percent of respondents were in favor of consumer education efforts. Sixty-three percent said applying new controls, such as authentication, to Internet-initiated payments was necessary. More than half of respondents were in support of the replacement of magnetic stripe technology. A similar number of respondents thought their organizations should share information about emerging fraud tactics.

With regard to new authentication methods, respondents favored multifactor authentication, followed by having a chip and PIN requirement and the use of a token. Biometrics was least favored out of a list that also included, among other methods, mobile device authentication, out-of-channel authentication and having a chip for dynamic authentication.

Finally, respondents were asked to offer their views on legal and regulatory changes that would help reduce payments fraud. The top choice for Fifth District respondents was increasing the penalties for fraud and attempted fraud. Respondents were deadlocked on the next two changes: placing more responsibility on consumers and customers to reconcile and protect their payments data; and placing the responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment.
Table 12 lists these suggestions.

Table 10: New Methods Needed by % of Respondents

	FI (N=75)	Non-FI (N=4)	All (N=79)
Consumer Education of Fraud Prevention	72%	0%	68%
Control Over Internet Payments	65%	25%	63%
Replacement of Card or Magnetic Stripe Technology	53%	50%	53%
Improved Methods of Info Sharing on Emerging Fraud Tactics	51%	75%	52%
Other	7%	0%	6%

Table11: New Authentication Methods Needed by % of Respondents

	FI (N=67)	Non-FI (N=4)	All (N=71)
Multifactor Authentication	64%	75%	65%
Chip and PIN Requirement	55%	75%	56%
Token (USB Token or Fob)	49%	0%	46%

Table 12: Legal and Regulatory Considerations by % of Respondents

	FI (N=73)	Non-FI (N=4)	All (N=77)
Increase penalties for fraud and attempted fraud	75%	25%	73%
Place more responsibility on consumers to reconcile and protect their data	71%	25%	69%
Place more responsibility on the entity that initially accepts the card	71%	25%	69%
Assign liability for losses to the party most responsible for not reducing risk	57%	50%	57%
Improve law enforcement cooperation	57%	25%	56%
Strengthen disincentives to committing fraud	53%	25%	52%
Align Regulation E & CC to reflect changes in the check collection systems	41%	25%	40%
Focus future legal or regulatory changes on data breaches to their source	36%	0%	34%
Establish new laws/regulations or change existing to strengthen framework	33%	0%	31%
Assign responsibility for mitigating fraud to the party best positioned to act	30%	0%	29%

Conclusions

All of the respondents to the Fifth District's 2012 Payments Fraud Survey experienced attempted or actual payments fraud during 2011. Some of the highlights of the report are:

- Despite rapid growth in the general purpose reloadable card market (prepaid cards), no respondents reported any significant fraud attempts or financial losses with this payment type.
- Signature debit cards are most problematic for the District's respondents, as this payment type had the highest number of fraud attempts, suffered the highest financial losses and was the chief contributor to the increase in fraud losses for respondents so affected in 2011. This is consistent with the findings from the overall survey including the other Reserve Banks and the Independent Community Bankers of America.
- The majority of organizations report total fraud losses equivalent to less than 0.3 percent of their annual revenue. While any loss is undesirable, this suggests that losses are relatively well managed. This was also in line with the responses from the Systemwide survey.
- Internal controls and procedures, such as periodic internal and external audits, are the main methods used by most organizations to mitigate payments fraud risk.
- Lack of staff resources is the main barrier to adding or upgrading fraud prevention measures faced by the District's respondents.
- Regarding new authentication methods, organizations preferred multifactor authentication followed by chip and PIN requirements and tokens.
- Respondents believed that increased penalties for fraud or attempted fraud was the main legal or regulatory change that would help reduce payments fraud.

---

[1] Questions regarding the survey summary may be directed to Neil Mitchell (Neil.Mitchell@rich.frb.org) or Pamela Rabaino (Pamela.Rabaino@rich.frb.org) at the Federal Reserve Bank of Richmond.

[2] This survey was conducted in conjunction with the Federal Reserve Banks of Minneapolis, Boston and Dallas and the Independent Community Bankers of America. Reserve Banks are publishing regional survey results, and highlights of the aggregate survey results will be available from the Federal Reserve Bank of Richmond's website.

[3] Thanks to Kiran Krishnamurthy of Corporate Communications for the tweet that went out during the survey.

[4] In the survey, most data collected was specific to 2011 while other data, e.g., mitigation services that respondents currently use, was as of survey date. For simplicity, 2011 is listed in the charts and tables even though some information may relate to a respondent's status as of April 2012.

[5] We are grateful to Steve Malone of District Outreach who provided us with their mailing list of Fifth District financial institutions.

[6] Signature debit, as the name suggests, refers to the processing of a debit card transaction solely with the provision of a signature by the card holder. This type of debit card transaction has a higher potential for fraud than a PIN-based debit transaction because of the method of verification: Signatures can be forged and are often not positively verified, whereas a PIN is either known or not. See http://portalsandrails.frbatlanta.org/2012/01/pin-authentication-vs-signature-authentication.html for recent research on the issue.