

2012 Payments Fraud Survey

Consolidated Results

Payments Information & Outreach Office Federal Reserve Bank of Minneapolis

September 25, 2012

Topics



- Survey Methodology & Respondent Profile
- Fraud Attempts & Losses
- Risk Mitigation
- Opportunities to Reduce Payments Fraud
- Conclusions



Survey Methodology & Respondent Profile

Payments Fraud Survey



- Sponsored by the Federal Reserve Banks of Minneapolis, Boston, Dallas, & Richmond & the Independent Community Bankers of America (ICBA)
- Conducted in April & May 2012
- Survey participants include financial institution (FI) & non-FI members of regional payment & treasury management associations & ICBA
- 740 respondents 93% were Fls, 7% were non-Fls

Respondent Size by Revenue



The majority of respondents (58%) are relatively small with annual revenues less than \$50 million



FI Respondents



FI Mix

689 Financial Institution (FI) respondents

FI Size by YE 2011 Assets



FI Payment Products Offered



Target Customers	Banks (N=592)	Credit Unions (N=66)	Thrifts (N=29)
Both consumers & business or commercial clients	88%	24%	62%
Primarily to consumers	6%	76%	38%
Primarily business or commercial clients	6%	0%	0%



Non-FI Respondents

 Non-FI respondents from more than 14 industries; 47% were larger organizations with annual revenues over \$1 billion





Non-FI Payment Types Used



 Over ¾ of businesses use check, ACH & wire payments

Typical Payment Counterparties	% of Non-Fls
Payments to/from both consumers & businesses	53%
Payments to/from other businesses	39%
Payments to/from consumers	8%





Payment Fraud Attempts & Losses

Fls Most Prone to Signature Debit Card Frauds



96% of FIs experienced payment fraud attempts & losses

Top 3 Payment Types with Highest # of Fraud Attempts & Losses % of FIs with Attempts or Losses



Non-FIs Most Prone to Check & Credit Card Frauds



 77% of non-FIs experienced payment fraud attempts & 46% experienced losses

> Top 3 Payment Types with Highest # of Fraud Attempts & Losses % of Non-FIs with Attempts or Losses



Fraud Losses & Trends



- 7% of respondents reported no fraud losses
- 69% of respondents estimated a financialloss rate of < 0.3% of revenues
- ~85% of respondents reported fraud losses increased or stayed the same in 2011

Loss Range as a % of Annual Revenue	% of FIs (N=631)	% of Non-Fls (N=43)	% of All Resp. (N=674)
0%	4%	54%	7%
Over 0% < 0.3%	72%	35%	69%
0.3% - 0.5%	14%	2%	13%
0.6% - 1.0%	7%	5%	6%
1.1% - 5.0%	4%	5%	4%
Over 5.0%	1%	0%	1%
Loss Rate	% of FIs (N=646)	% of Non-Fls (N=43)	% of All Resp. (N=689)
Increased	51%	9%	48%
Stayed the Same	34%	67%	36%
Decreased	16%	23%	16%

Column values may not add to 100% due to rounding

Prevention Costs Versus Actual Fraud Losses





©2012 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

For most payment types, investments in fraud prevention exceed actual losses with two exceptions:

- 1) Debit signature
- 2) Mobile payments

Increased Fraud Losses



- Half of the respondents with increased losses reported their loss rate up in 2011 by 1% to 5% compared to 2010
- Increased losses were most
 common among
 card payments



Decreased Fraud Losses



- ~30% of respondents that reduced fraud losses cut their loss rate by over 10%
- Reduced losses were most common among payments most vulnerable to
 fraud attempts & losses—cards & checks



Payment Types with Decreased Losses



Reducing Fraud Losses



 68% of respondents said key changes in risk management practices led to decline in losses

Key Changes Made	FIs (N=68)	Non-Fls (N=6)	All (N=74)	
Enhanced fraud monitoring system	72%	50%	70%	
Staff training & education	62%	83%	64%	
Enhanced internal procedures & controls	46%	67%	47%	
Adopted/increased use of risk management tools offered by financial service provider	43%	50%	43%	
Enhanced method to authenticate customer &/or validate customer account	31%	50%	32%	



Perpetrators



 External parties were most often responsible for successful fraud attempts

Portion of Successful Payments Fraud by Perpetrators Involved (% of Respondents)

	100%	76% - 99%	51% - 75%	26% - 50%	1% - 25%
Internal Only	2%	2%	2%	4%	4%
Internal w/External Parties	3%	0%	1%	5%	4%
External Only	58%	7%	2%	3%	4%
Could Not Determine	8%	1%	1%	2%	6%

71% of respondents attributed all successful fraud to a single perpetrator category

29% of respondents attributed a portion of successful fraud to more than one perpetrator category

Fraud Schemes Involving FI Customers' Accounts



 Most used schemes are counterfeit or stolen cards used at POS or online



Top 3 Most Used Schemes (% of FIs)

Fraud Schemes Involving Payments Accepted by Non-Fls



 Most used schemes involve checks—altered, forged & counterfeit



Top 3 Most Used Schemes (% of Non-FIs)

Fraud Schemes Involving Organization's Own Banking Accounts



 Most used schemes involve checks—altered, forged & counterfeit



Top 3 Most Used Schemes (% of Respondents)

Source of Data Used in Schemes



Top 3 Information Sources Used in Fraud Schemes	Fls (N=590)	Non-Fls (N=33)
"Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control	64%	39%
Physical device tampering e.g., use of skimmer on POS terminal or obtaining magnetic stripe information	38%	3%
Email and webpage cyber attacks e.g., phishing, spoofing & pharming to obtain "sensitive" customer information	33%	21%
Data breach due to computer hacking or cyber attacks	26%	15%
Information about customer obtained by family or friend	24%	3%
Organization's information obtained from a legitimate check issued by your organization	17%	67%
Lost or stolen physical documentation or electronic devices while in control of the organization	3%	9%
Employee with legitimate access to organization or customer information	1%	18%



Risk Mitigation

Internal Controls & Procedures Use by Fls

Over 80% of FIs use 12 of 15 internal controls

Periodic internal/external audits Address exception items timely Dual controls/separate duties w/in pymt processes Verify controls applied via audit or mgmt review Reconcile bank accounts daily Authentication/authorization controls-pymt process Logical access controls to network/pymt apps Review card-related reports daily Transaction limits for payment disbursements Physical access controls to pymt processing functions Restrict/limit staff use of Internet via org's network Transaction limits for corporate card purchases Separate banking accts by purpose or pymt type Dedicated computer for trxs w/ FI or FS provider Employee hotline to report potential fraud

> Plan to Use by 2014 Use



DESERVE BANK

Internal Controls & Procedures Effectiveness Rated by FIs Using

95%+ rate all as effective; 55% to 80% rate as very effective

accounts daily		8	2%		18%	0%
ent processes		8.	1%		19%	0%
or FS provider 「		8.	1%		18%	1%
/mt processes		80	%		20%	0%
payment apps		79	%		21%	0%
n items timely		77	%		22%	0%
sing functions		76%	0		24%	0%
xternal audits		74%	0		26%	0%
mgmt review		71%			29%	0%
lisbursements		71%			29%	0%
d reports daily		71%			29%	0%
ard purchases		69%			31%	1%
or pymt type		68%			31%	2%
otential fraud		65%		32	2%	4%
org's network		55%		43%		2%
0	% 20	% 40)% 60	80)%	100%
Somewhat ef	fective	Somewha	it ineffectiv	e N	=220 to	530

Reconcile bank accounts daily Dual control/separate duties w/in payment processes Dedicated computer to conduct trx w/FI or FS provider Authentication/authorization controls to pymt processes Logical access controls to network/payment apps Address exception items timely Physical access controls to pymt processing functions Periodic internal/external audits Verify controls applied via audit or mgmt review Transaction limits for payment disbursements Review card-related reports daily Transaction limits for corporate card purchases Separate banking accounts by purpose or pymt type Employee hotline to report potential fraud Restrict/limit employee Internet use from org's network

Very effective

HANK OF HILL ENDLY

Internal Controls & Procedures Use by Non-FIs

Over 80% of non-FIs use 8 of 15 internal controls

0% 97% 0% 97% 94% 0% 3% 94% 94% 0% 3% 91% 3% 88% 3% 85% 79% 3% 0% 79% 73% 3% 65% 3% 56% 3% 3% 49% 41% 9%

Physical access controls to pymt processing functions Dual controls/separate duties w/in pymt processes Periodic internal/external audits Authentication/authorization controls-pymt process Logical access controls to network/pymt apps Transaction limits for corporate card purchases Verify controls applied via audit or mgmt review Address exception items timely Reconcile bank accounts daily Transaction limits for payment disbursements Separate banking accts by purpose or pymt type Restrict/limit staff use of Internet via org's network Employee hotline to report potential fraud Dedicated computer for trx w/ FI or FS provider Review card-related reports daily

N=32 to 35

Use Plan to Use by 2014

Internal Controls & Procedures Effectiveness Rated by Non-FIs Using



·]			100%	, ,			0%	60%
· -			96%				4%	0%
			94%				7%	0%
			93%				7%	0%
, -			93%				7%	0%
_			87%			13	3%	0%
-		c	2%			170		070 %
		0	10/			1.00/		/0 0/
-		0	170			19%	5 07	70 D/
-		/5	1%			21%	0	%
-			~			23%	0	%
· _		739				27%	09	%
_		73%	9			23%	5%	I
		72%	5			28%	0	%
		62%			- 38	8%	0	%
		50%			44%		6%)
0%	20)% 4(0%	60%	80)%	100)%
effect	ive	Somewha	at ineffe	ctive] N	=11 to 3	31	

Review card-related reports daily Reconcile bank accounts daily Authentication/authorization controls to pymt processes Dual control/separate duties w/in pymt processes Address exception items timely Physical access controls to pymt processing functions Logical access controls to network/payment apps Periodic internal/external audits Verify controls applied via audit or mgmt review Transaction limits for corporate card purchases Dedicated computer to conduct trx w/FI or FS provider Separate banking accounts by purpose or pymt type Transaction limits for payment disbursements Restrict/limit employee Internet use from org's network Employee hotline to report potential fraud

Very effective

©2012 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Somewhat

Customer Authentication Methods Use by FIs

Over 60% of FIs use 7 of 10 methods; 12% plan to adopt card chip authentication by 2014

PIN authentication 91% 1% 84% 3% 81% 1% 2% 1% 66% 8% 2% 5% 21% **6%** 3% Card chip authentication 2%12%

Signature verification Customer authentication for online transactions Verify CID codes on payment card Magnetic stripe authentication Real-time decision support during acct appl or POS Positive ID of purchaser for in-store/person trx Verify customer ID is authentic (magnetic stripe) Biometrics authentication

Use Plan to Use by 2014

N=502 to 557

©2012 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.



1%

Customer Authentication Methods Effectiveness Rated by FIs Using

Biometrics, PIN, positive ID & online authentication rated very effective by $\sim 2/3$ of FIs that use them



Positive ID of purchaser for in-store/person trx Customer authentication for online transactions Real-time decision support during acct appl or POS Verify customer ID is authentic (magnetic stripe) Verify CID codes on payment card Magnetic stripe authentication

©2012 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

ALSERVE BANK

Customer Authentication Methods Use by Non-FIs

 Over 30% of non-FIs use 4 of 10 methods; 13% plan to adopt card chip authentication by 2014

Customer authentication for online transactions Verify CID codes on payment card Signature verification Positive ID of purchaser for in-store/person trx PIN authentication Real-time decision support during acct appl or POS Magnetic stripe authentication Verify customer ID is authentic (magnetic stripe) Card chip authentication



Use Plan to Use by 2014

Customer Authentication Methods Effectiveness Rated by Non-FIs Using



All non-FIs that use PIN or card-chip authentication rate them as very effective

PIN authentication Card chip authentication Real-time decision support during acct appl or POS Customer authentication for online transactions Magnetic stripe authentication Verify CID codes on payment card Positive ID of purchaser for in-store/person trx Signature verification Verify customer ID is authentic (magnetic stripe) Biometrics authentication 0% 20%

100% 0% 100% 0% 75% 25% 0% 65% 35% 0% 25% 50% 25% 47% 40% 13% 40% 60% 0% 73% 0% 75% 0% 20% 40% 60% 80% 100% Somewhat effective Somewhat ineffective N=2 to 17

Transaction Screening & Risk Mgmt Methods Use by FIs



Over 60% of FIs use 6 of 9 methods; 10% of FIs plan to adopt 3 of the methods by 2014

Provide staff edu. on pymt fraud risk mit. Fraud detection pen for currency Human review of payment transactions Participate in fraudster databases & receive alerts Provide customer edu. on pymt fraud risk mitigation Fraud detection software w/ pattern matching Centralized risk management department Centralized fraud info database - one pymt type Centralized fraud info database - mult pymt types



Use Plan to Use by 2014

N=522 to 564

Trx Screening & Risk Mgmt Methods Effectiveness Rated by FIs Using

 Centralized risk mgmt & fraud detection software rated very effective by ~60% of FIs that use them

Centralized risk management department Fraud detection software w/ pattern matching Centralized fraud info database - mult pymt types Centralized fraud info database - one pymt type Fraud detection pen for currency Human review of payment transactions Provide staff edu. on payment fraud risk mit. Participate in fraudster databases & receive alerts Provide customer edu.on payment fraud risk mit.

Very effective



ASSERVE BANK

Transaction Screening & Risk Mgmt Methods Use by Non-Fls



 Over 50% of non-FIs use 3 of 9 methods; 6% -9% plan to provide customer & staff education by 2014

Human review of payment transactions Provide staff edu. on pymt fraud risk mit. Centralized risk management department Fraud detection pen for currency Fraud detection software w/ pattern matching Provide customer edu. on pymt fraud risk mit. Participate in fraudster databases & receive alerts Centralized fraud info database - one pymt type Centralized fraud info database - mult pymt types



N=31 to 35

©2012 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Use

Trx Screening & Risk Mgmt Methods Effectiveness Rated by Non-FIs Using



 7 of 9 methods rated as very effective by ½ of the non-FIs that use them

Centralized fraud info database - mult pymt types Fraud detection software w/ pattern matching Centralized fraud info database - one pymt type Human review of payment transactions Provide staff edu. on payment fraud risk mit. Provide customer edu.on payment fraud risk mit. Participate in fraudster databases & receive alerts Centralized risk management department Fraud detection pen for currency

Very effective



FI Risk Services Use by Non-FIs

- THE DISTRICT OF THE REAL PROPERTY OF THE REAL PROPE
- 60% of non-FI respondents use 8 of 13 risk services offered by FIs; ACH risk services are highest among services companies plan to adopt by 2014



FI Risk Services Effectiveness Rated by Non-FIs Using

 All positive pay, payee positive pay & acct masking services rated very effective by 90%+ of companies using them



FI Risk Services Offered by FIs & FS Providers



 Over 85% of the FIs offer the two services used by most businesses surveyed; 50% of the FIs offer 5 of the 13 services



Barriers to Reducing Payments Fraud



 Most identified some aspect of "cost" as the main barrier

Barriers	Fls	Non-Fls	All
Lack of staff resources	56%	70%	57%
Consumer data privacy issues/concerns	39%	33%	39%
Cost of implementing in-house fraud detection tool/service	39%	7%	37%
Cost of implementing commercially available fraud detection tool/service	38%	19%	37%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	37%	48%	37%
Corporate reluctance to share information due to competitive issues	15%	22%	15%
Unable to combine payment information for review due to operating w/ multiple business areas, states or banks	15%	19%	15%



Opportunities to Reduce Payments Fraud

New Methods Needed



New or Improved Methods Most Needed	Fls (N=537)	Non-Fls (N=32)	All (569)
Controls over Internet payments	66%	41%	65%
Replacement of card/magnetic stripe technology	62%	31%	60%
Consumer education on fraud prevention	62%	47%	61%
More aggressive law enforcement	51%	41%	50%
Information sharing on emerging fraud tactics being conducted by criminal rings	45%	63%	46%
Controls over mobile payments	45%	44%	44%
Industry specific education on best prevention practices for fraud	34%	28%	34%
Industry alert services	29%	31%	29%
Image survivable check security features for biz checks	16%	19%	16%

Authentication Adoption Methods Preferred



- Majority favor a "Chip & PIN" requirement & multi-factor authentication
- Adoption of EMV technology (Chip) is just getting underway in the U.S.

Authentication Method Preferences	Fls	Non-Fls	All
Chip & PIN requirement	60%	39%	59%
Multi-factor authentication	57%	46%	56%
Chip for dynamic authentication	43%	31%	42%
PIN requirement	39%	42%	39%
Out-of-band/channel authentication to authorize payment	38%	15%	37%
Token	38%	62%	39%
Mobile device to authenticate person	28%	27%	27%
Biometrics	24%	8%	23%

Legal or Regulatory Change



- Top three changes identified by respondents that would help reduce payments fraud:
 - Place responsibility to mitigate fraud & shift liability for fraudulent card payments to the entity that initially accepts the card payments
 - Increase penalties to perpetrators for attempted & successful fraud
 - Place more responsibility on consumers & customers to reconcile & protect their payments data



Conclusions

Conclusions



- Considered as a whole, the 2012 payments fraud survey results suggest the following:
 - Payments related fraud remains a significant concern of FIs & others
 - For FIs, signature debit card is the payment instrument most vulnerable to attempted fraud & FI losses
 - Over half of FIs reported that signature debit card losses from fraud exceeded their investment in mitigation to prevent such fraud; this seems to suggest a cost-effective opportunity to increase these fraud prevention investments

Conclusions (continued)



- For non-FIs, check continues to be the payment instrument most vulnerable to attempted fraud & losses
- Corporate account take-over can result in significant losses, but it was not identified as a commonly occurring fraud scheme that affected a high percentage of respondents to this survey
- Most FIs & others report total fraud losses that represent less than 0.3% of their annual revenues
- Strategies to detect & prevent fraud effectively require the use of multiple mitigation methods & tools – i.e., a "layered" strategy

Conclusions (continued)



- Two-thirds of respondents that reduced their fraud losses cited enhanced fraud monitoring systems & employee education & training
- Offering risk mitigation services to customers is a growing area of opportunity for FIs
- Cost is the main barrier that prevents FIs & others from investing more in mitigating payments fraud
- FIs & others are focused now on the need for alternatives to magnetic stripe authentication technology to secure card payments



Regional Survey Results

Regional Survey Results



Federal Reserve Bank Contacts

Marianne Crowe Federal Reserve Bank of Boston **Payment Strategies** http://www.bostonfed.org/bankinfo/payment-strategies/index.htm Matt Davies Federal Reserve Bank of Dallas **Financial Institution Relationship Management** http://www.dallasfed.org/banking/firm/fi.cfm Claudia Swendseid or Amanda Dorphy Federal Reserve Bank of Minneapolis **Payments Information & Outreach Office** http://www.minneapolisfed.org/about/whatwedo/paymentsinformation.cfm Pamela Rabaino Federal Reserve Bank of Richmond **Payments Studies Group** http://www.richmondfed.org/