2017 Financial Institution Payments Fraud Mitigation Survey

Report of Results

Amanda Dorphy and Heather Hultquist
Payments, Standards, and Outreach Group
Federal Reserve Bank of Minneapolis

January 2018

Table of Contents

The authors thank colleagues at the Federal Reserve Banks of Minneapolis and Chicago for their assistance in preparing the survey and this report. The views expressed in this report are those of the authors and are not necessarily those of the Federal Reserve Bank of Minneapolis or any other component of the Federal Reserve System. The information in this report is intended for educational purposes and the description of survey results, or the mention or display of a trademark, proprietary product, or firm in this report does not constitute an endorsement or criticism and does not imply approval to the exclusion of other suitable products or firms.

Executive Summary

Staff at the Federal Reserve Bank of Minneapolis have conducted research on payments fraud mitigation since 2007. During July and August 2017, the Federal Reserve Bank of Minneapolis' Payments, Standards, and Outreach Group fielded a qualitative, online survey of financial institutions (FIs) from across the U.S. on payments fraud mitigation. There are 283 respondents, representing about a 5.8% response rate.

The survey report contains information about the most frequent fraud attacks by payment type – debit card, credit card, check, ACH, and wire – that FIs are experiencing and the usage and relative effectiveness of payments fraud mitigation methods. Risk mitigation methods for each payment type are grouped into three categories:

1. transaction screening/scoring,
2. authentication methods, and
3. other reporting and risk management methods.

Aggregate results are presented in the first half of this report. On each page, summary remarks, the question posed in the survey, and a chart reflecting results are provided. Data tables shown in the second half of the report provide results by financial institution size. A copy of this report and definition of terms used in the survey may be found on the Federal Reserve Bank of Minneapolis' Payments, Standards, and Outreach Group website.

Key Findings

General

- Payment fraud losses continue to be a problem for FIs: three out of four survey respondents report incurring fraud losses.
- Nearly all FIs *provide customers access to online information services to view transactions, statements, etc*. The effectiveness rating of online information services in mitigating fraud is somewhat high. About half of the FIs rate it as very effective. This rating applies to all payment types, even wire transfers where speed and finality are a core feature. This finding seems to indicate that when other methods fail, the customer is relied on to identify fraudulent transactions. At the same time many FIs *provide customer education on fraud mitigation*; however, this is rated low in effectiveness.

Executive Summary

Cards

- Ninety-six percent of the respondents that are debit card issuers and 77% of credit card issuers experienced card fraud losses in 2016. Increases in losses are more prevalent on debit and credit cards compared to other payment types. Fraud losses increased in 2016 compared to 2015 on debit cards (63% of FIs) and credit cards (41% of FIs).
- The most frequent card fraud attacks are *counterfeit cards used at point-of-sale* and *fraudulent use of account numbers online*. Eighty-one percent of the FIs that offer debit cards and 91% of the FIs that offer credit cards stated they have adopted chip card technology. Use of chip technology is a method to help thwart counterfeit card fraud attacks at point-of-sale.
- For card transactions (debit and credit), 70% of respondents use seven of 11 data types listed in the survey in their fraud screening and scoring tools, indicating a layered approach is being applied. *Identifying transactions initiated in countries perceived as high risk* is considered a key data type in screening/scoring transactions and is rated most effective. Other data with high adoption rates are rated moderately effective.

Checks

- Seventy-seven percent of FIs that offer check experienced fraud losses in 2016.
- The three most frequent check fraud attacks are *altered or forged checks presented for payment*, *counterfeit checks presented for payment*, and *counterfeit checks deposited*.
- Two-thirds of FIs use five of the 11 check fraud screening and scoring methods. Of those five methods, only 42% of FIs under $50 million in assets use *duplicate check detection on deposit or paid items* compared to over 70% by FIs in other size categories. More than 80% of FIs use funds availability holds with half rating the *application of exception holds on funds availability* as very effective and 40% reporting the same for *routinely applying standard check holds*.

ACH

- Twenty-four percent of FIs that offer ACH experienced fraud losses in 2016.
- Eight out of 10 FIs rank *fraudulent or unauthorized debits against consumer accounts* as the number one most frequent attack. *Fraudulent or unauthorized debits against business accounts* is ranked second.
- *Manual review* processes are used by over 80% of FIs. Nearly half the FIs using *manual review* processes rate them as very effective. Screening for *anomalous behavior* has a higher use rate by large FIs (74% of those $1 billion or more in size) and is rated very effective by four out of 10 large FIs.

Executive Summary

Wire

- Thirteen percent of FIs that offer wire experienced fraud losses in 2016.
- *Business email compromise (BEC)* attacks and *consumer-victim frauds* (frauds targeting consumers) are identified as the most frequent wire fraud attacks. However, for small FIs (under $50 million in assets) none of the respondents rank BEC attacks first or second and only 5% rank them third as a most frequent attack. In contrast, 74% of the largest FIs (over $1 billion in assets) rank BEC attacks number one and 91% indicate it is in the top three.
- Three of the nine authentication methods for wire transfers that are listed in the survey are used by over 80% of FIs, and over all these are rated as very effective. The top three are *telephone callback verification*, *dual control/approval for originating company wire initiation*, and *signature verification*. Although adoption is somewhat lower on *limiting consumer wires to in-person requests with a valid government ID* and *multifactor authentication with originating company*, these methods are rated high in terms of effectiveness. Given the top attacks identified, some of the less used authentication methods might help mitigate these attacks.
- Although consumer-victim frauds are a concern, 7% of respondents won't *refuse to send a consumer-initiated wire even when the FI suspects a fraud scheme.*

Barriers and Opportunities to Mitigate Payments Fraud

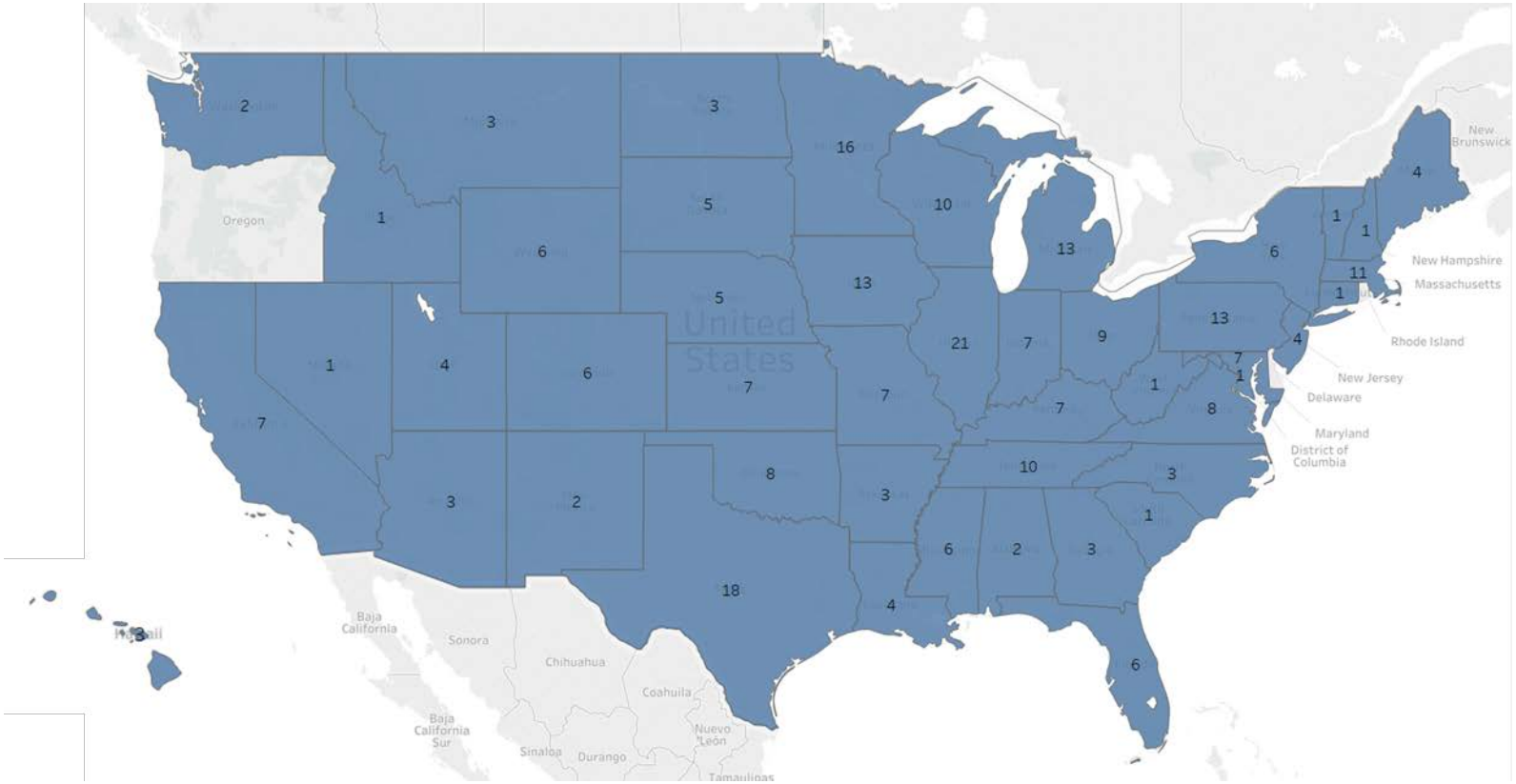
- From a list of six potential barriers, the top two constraints are *costs to implement fraud detection tools/methods* and *consumer data privacy regulatory restrictions/other concerns if data shared with others to help mitigate fraud*.
- Respondents answered an open-ended question on what new and improved methods are needed to help mitigate payments fraud. Opportunities relate to the following five themes are raised most:
  - Improved information sharing
  - Identity verification
  - Improved automation and analytics
  - Stakeholder liability changes
  - Increased adoption of existing methods

Respondent Demographics

Respondent Demographics

283 banks and credit unions headquartered across the country responded to the survey[1].

Respondents by State Location of Head Office



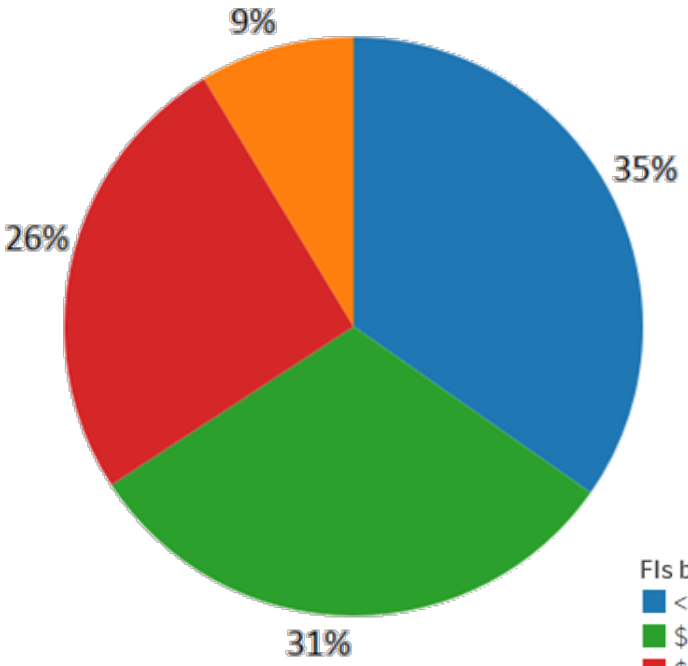
[1] References to banks in the report include cooperative banks, federal savings banks, national banks, state nonmember banks, savings and loan associations, state member banks, and state savings banks. Credit unions include federal credit unions and state credit unions.

Respondent Demographics – Correlate to U.S.

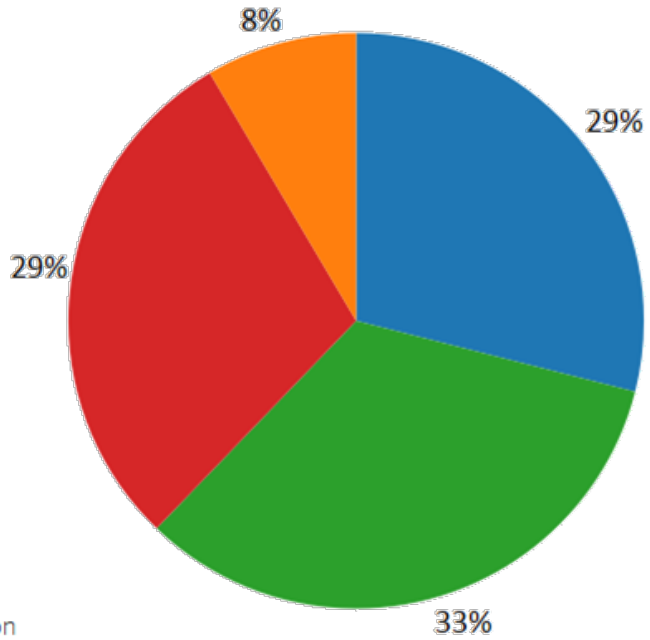
The mix of respondents based on size (total assets) is a **close match and reflective of FIs in the U.S.**

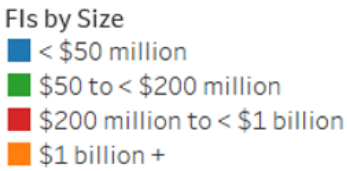
Financial Institutions (FIs) by Size
2016 YE Total Assets

U.S. Nationwide



Survey Respondents



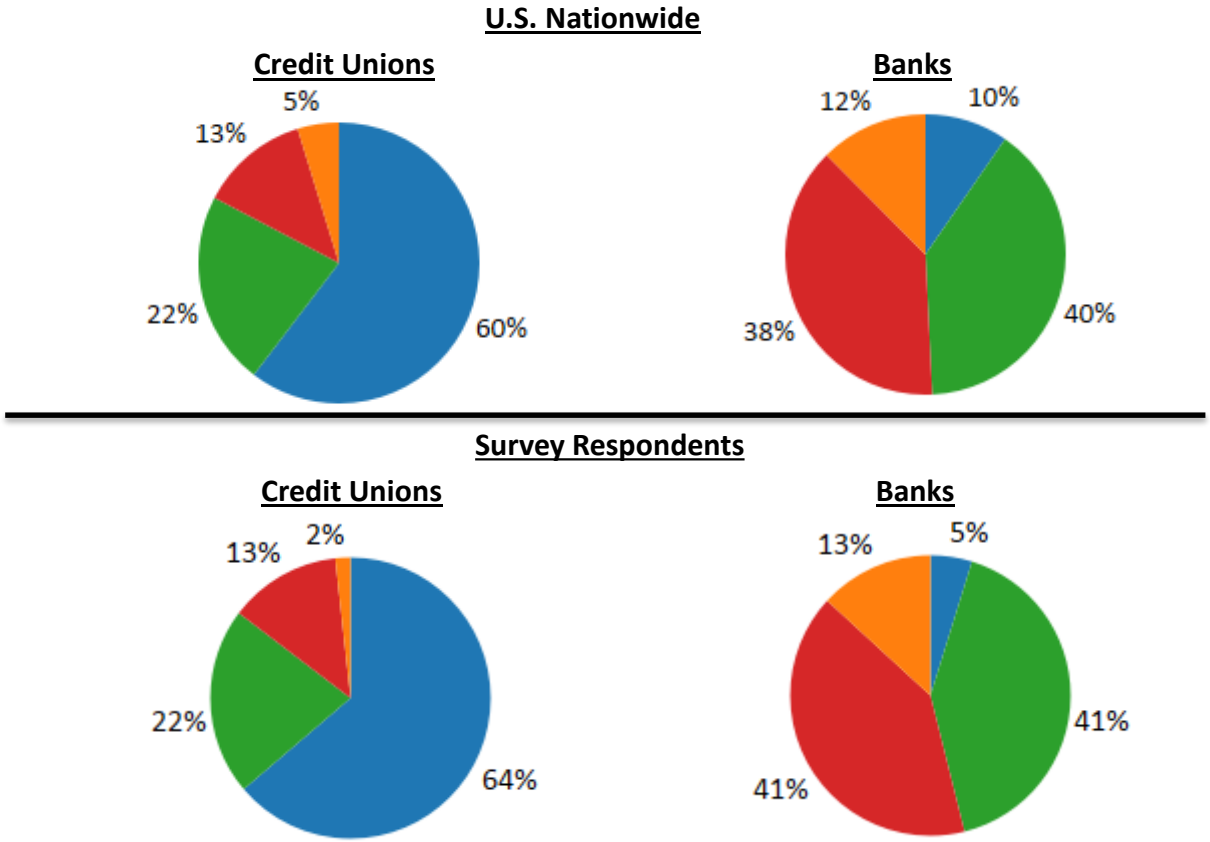


Source for national data: National Information Center (NIC) Call Report Data

Respondent Demographics

Nationally and among survey respondents, the majority of those under $50 million in assets are credit unions.

Financial Institutions by Type and Size
2016 YE Total Assets



Source for national data: National Information Center (NIC) Call Report Data

Customers Served by Respondent FIs

Seventy percent of respondents said the primary users of their payment products are consumers. This includes all of the credit union respondents, which make up 41% of the survey participants.

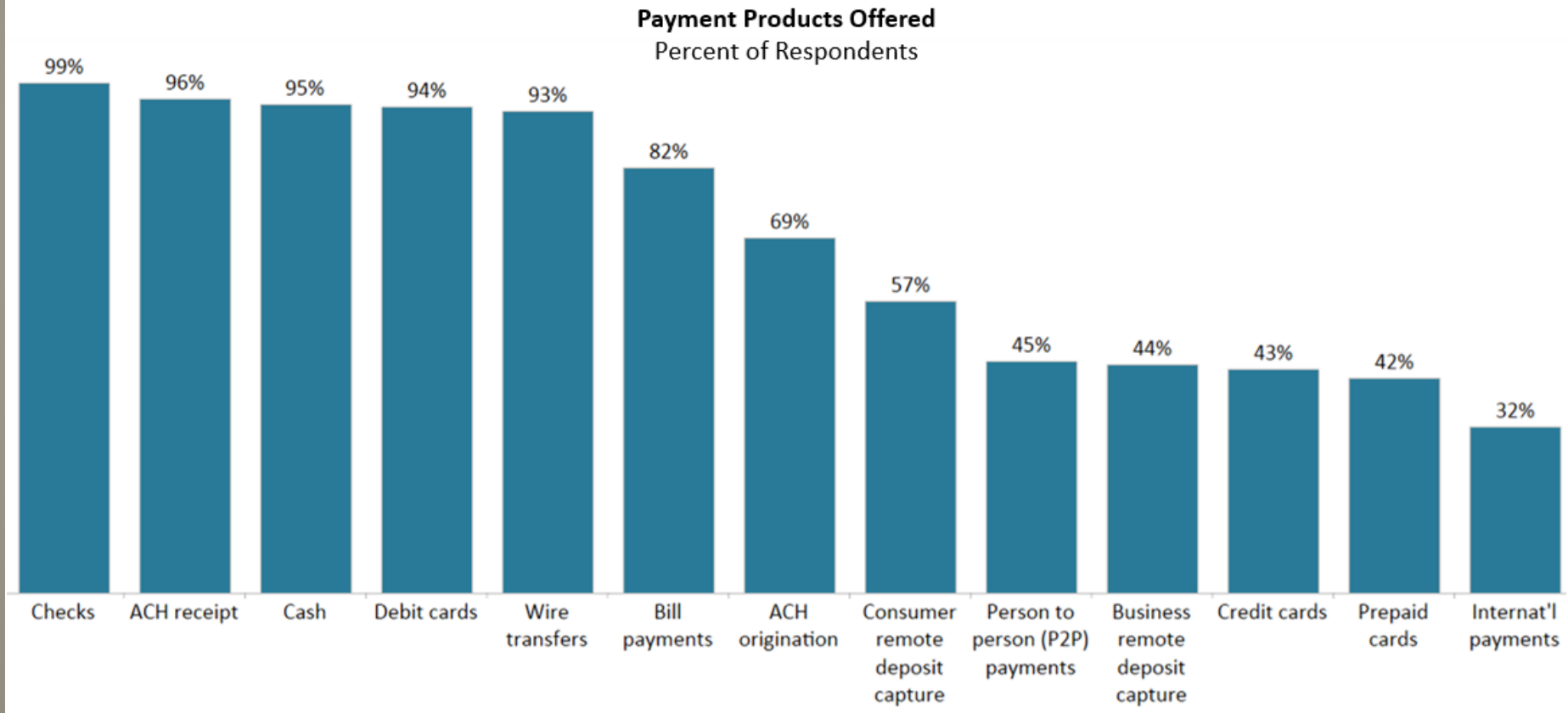
What type of customers are the predominant users of your financial institution's payment products and services?

Customer Type	Percent of Respondents
Primarily consumers	70%
Primarily business/commercial	5%
Both, somewhat even	25%

Payment Products Offered by Respondent FIs

Traditional payment products except credit cards are offered by most financial institutions. Only 43% of respondents offer credit cards, which for purposes of the survey, is defined as issuing cards and carrying the associated accounts receivable.

Which of the following payment products does your financial institution offer?



Payment Fraud Trends

Payment Fraud Attempts and Losses

A greater portion of smaller FIs, those under $50 million in assets, reported no payment fraud attempts (38%) and no fraud losses (45%). Whereas, over 80% FIs in all other asset-size segments reported that they experienced payment fraud attempts and losses.

Did your financial institution experience any payment fraud attempts and losses in 2016?

Fraud Attempts	*Respondent Size - Total Assets in Millions of Dollars*				
	All	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Yes	82%	57%	88%	95%	100%
No	16%	38%	11%	4%	-
Don't know	2%	5%	1%	1%	-

Fraud Losses	*Respondent Size - Total Assets in Millions of Dollars*				
	All	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Yes	75%	46%	85%	83%	100%
No	22%	45%	13%	14%	-
Don't know	4%	9%	2%	2%	-

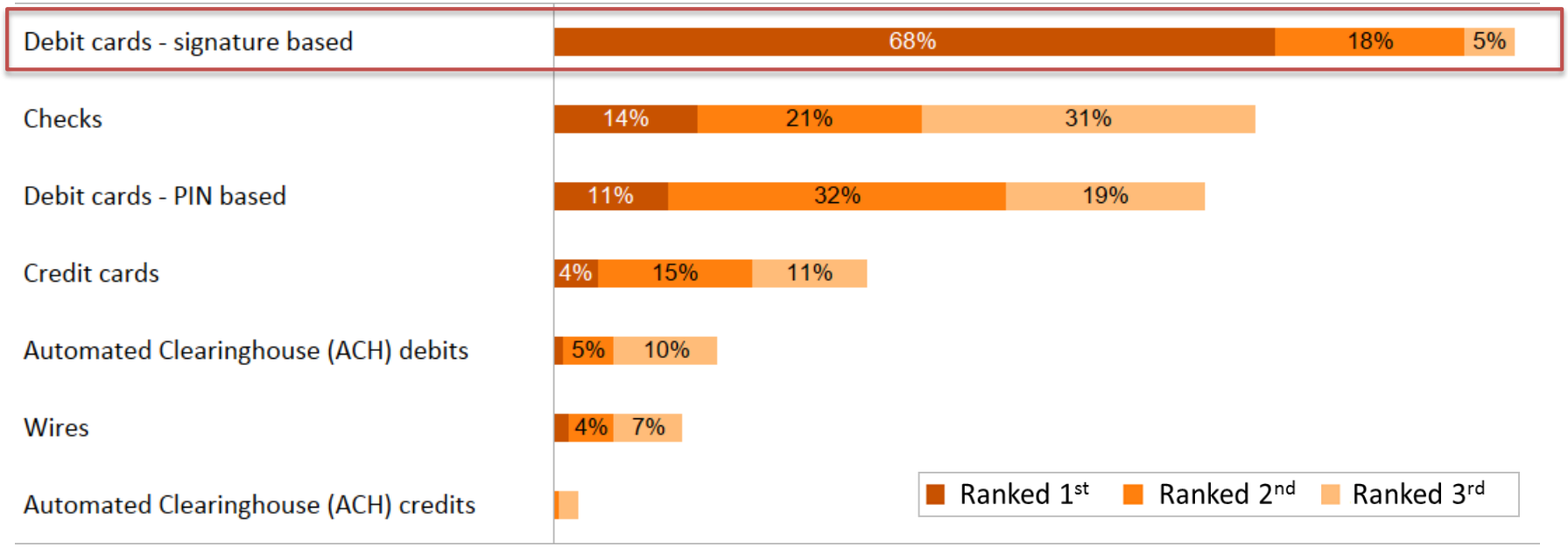
Payment Fraud Attempts

Over 90% of the respondents that track fraud attempts ranked signature-based debit cards among the top three payments having the highest number of fraud attempts. Sixty-six percent of respondents state check fraud attempts are in the top three payment types having the highest number of fraud attempts.

Although credit cards are fourth on the chart below, this does not imply that credit cards experience less fraud attempts compared to other payments. Only 43% of respondents offer credit cards.

Indicate the payment types where your financial institution experienced the highest number of fraud attempts in 2016. Consider all attempts regardless of actual financial losses.

Results for All Respondents



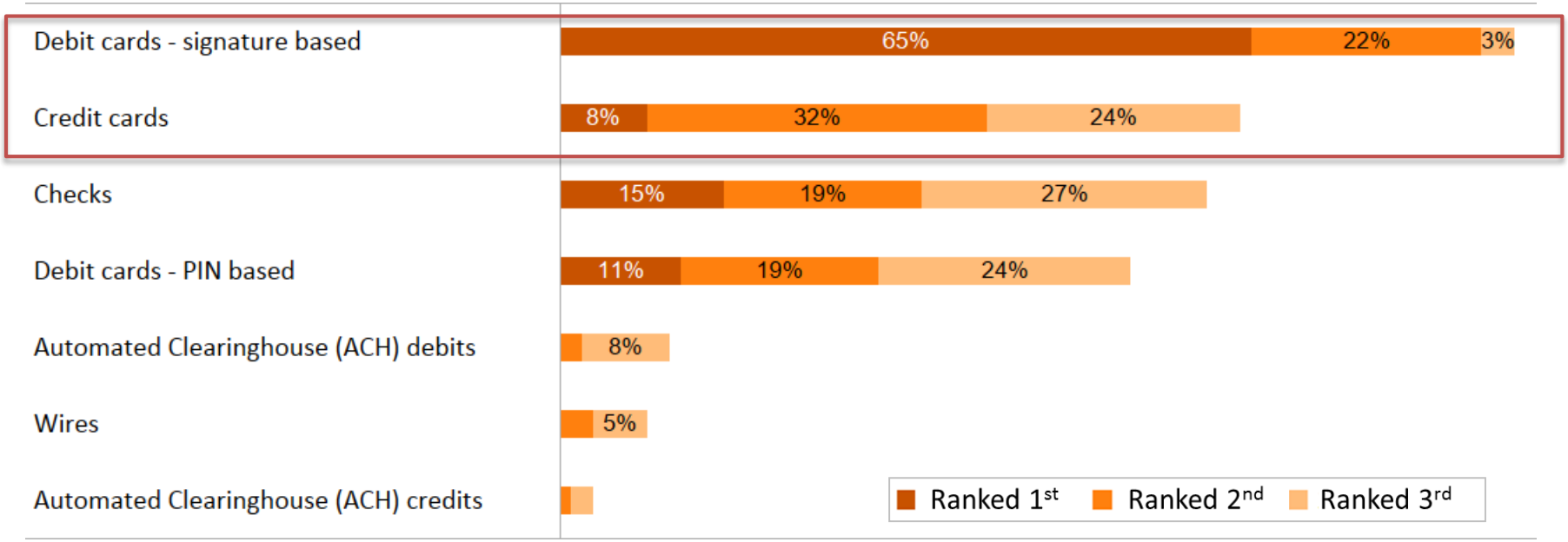
FIs are only asked about the payment types they offer.

Payment Fraud Attempts by Those That Offer Credit and Debit Cards

While only 43% of the respondents offered credit cards, for those that do (chart below), credit cards are cited in the top three payments with the highest number of fraud attempts by 64% of institutions surpassing both PIN debit and checks. However, signature-based debit cards are still reported as having the highest number of fraud attempts.

Indicate the payment types where your financial institution experienced the highest number of fraud attempts in 2016. Consider all attempts regardless of actual financial losses.

Results for FIs That Offer Credit and Debit



FIs are only asked about the payment types they offer.

Payment Fraud Losses

As discussed on page 13, three out of four of the survey respondents incurred fraud losses. FIs that experienced any payments fraud losses are asked about losses associated with the payments they offer:

- Over 75% of FIs experienced card fraud losses. Although PIN authentication is viewed as very effective, four out of five FIs still have PIN-based debit card losses.
- Check losses are common too; 74% of FIs have reported check fraud losses. However, only 48% of respondents under $50 million in assets reported check fraud losses.
- Less than 25% of FIs have ACH, wire, and prepaid cards fraud losses. A notable difference, 57% of large FIs (those over $1 billion in size) report ACH debit fraud losses.

On which payment types did fraud losses occur?

	Losses	No Losses	Don't Know
Debit cards - signature based	96%	2%	2%
Debit cards - PIN based	81%	14%	5%
Credit cards	77%	16%	7%
Checks	74%	23%	3%
Automated Clearinghouse (ACH) debits	23%	69%	8%
Wires	13%	84%	3%
Automated Clearinghouse (ACH) credits	8%	86%	6%
Prepaid cards	7%	86%	7%

FIs that incurred any payments fraud losses are asked about losses on payment types they offer.

Payment Fraud Losses: 2016 Compared to 2015

FIs reported fraud loss increases on multiple payment types. Increases are more prevalent on debit and credit cards. Although the number of checks written has dropped precipitously over the last decade[2], 28% of respondents saw growth in check fraud losses.

For your financial institution, how have losses due to payments fraud changed in 2016 compared to 2015?

	Increased	Stayed the Same	Decreased	Don't Know
Debit cards - signature based	63%	19%	15%	4%
Debit cards - PIN based	50%	33%	12%	6%
Credit cards	41%	32%	16%	11%
Checks	28%	47%	20%	5%
Wires	10%	77%	3%	10%
Automated Clearinghouse (ACH) debits	8%	79%	4%	8%
Prepaid cards	6%	76%		18%
Automated Clearinghouse (ACH) credits	2%	83%	4%	12%

FIs are only asked about the payment types they offer.

[2]Source Federal Reserve Payments Study, 2016 and 2013.

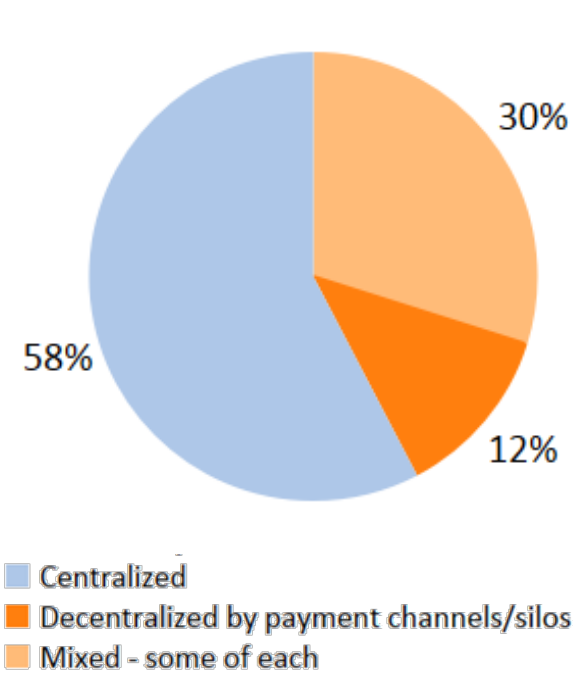
Payments Fraud Mitigation

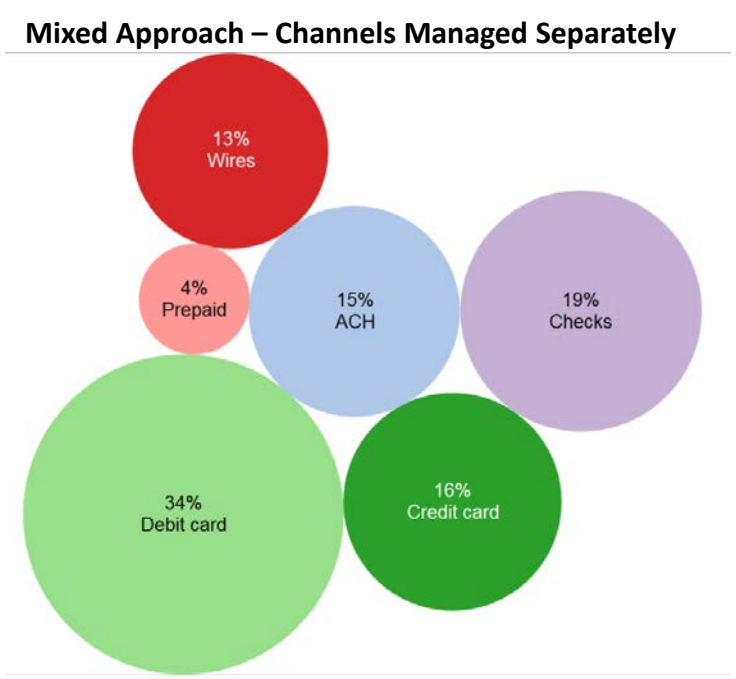
Fraud Prevention Approach

A centralized approach to fraud prevention and investigation is used by 58% of respondents, meaning they concentrate authority for managing fraud risk and associated activities in one area. Twelve percent use a decentralized approach where fraud risk is managed independently for each payment channel. Lastly, 30% of the FIs take a mixed approach. Cards are the most common payment where fraud risk is managed separately.

Large FIs (those over $1 billion in assets) manage fraud differently, with 33% reporting centralized, 17% reporting decentralized, and 50% reporting a mixed approach.

At your financial institution is fraud prevention/investigation a centralized function, is it decentralized by payment channel/silo, or is it some of each? (left chart) If mixed, which payment channels are managed separately? (right chart)



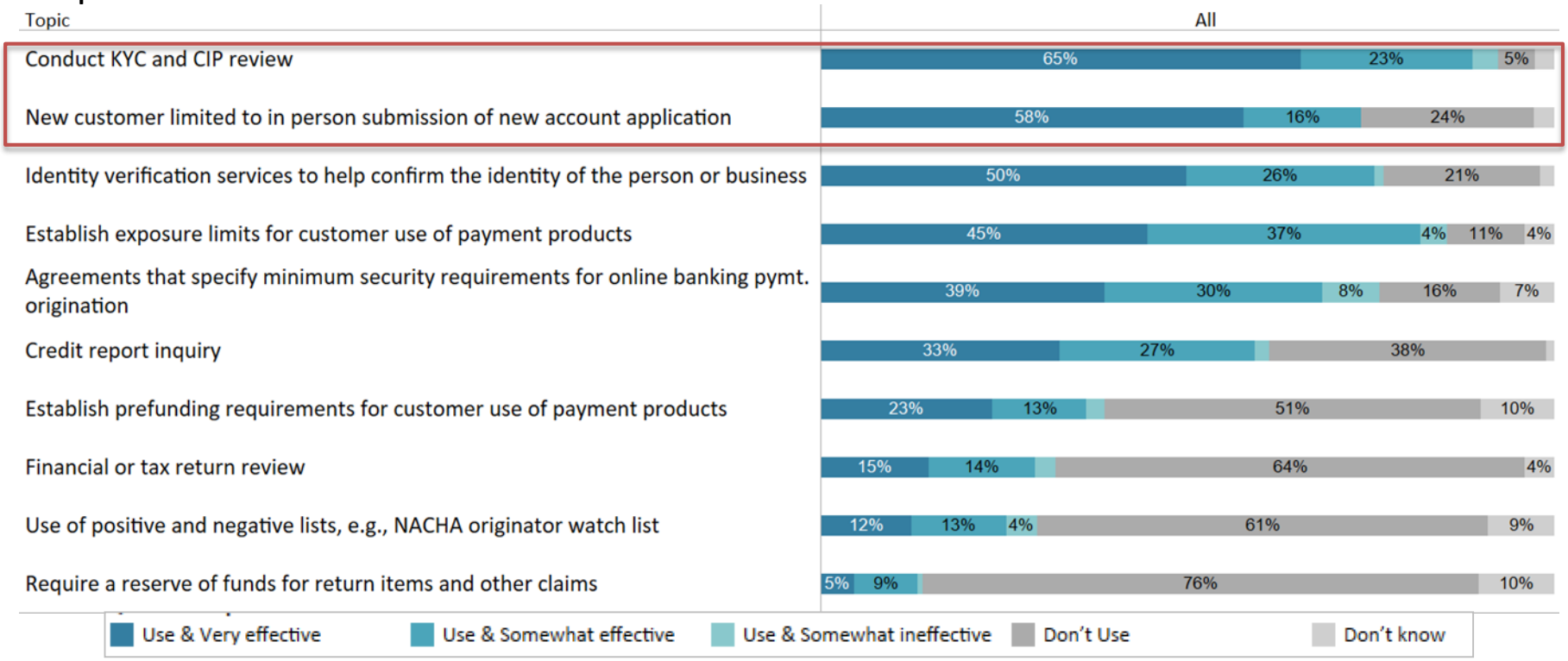


Account Application Processes

New Deposit Account Fraud Mitigation

Conduct know your customer (KYC) and customer identification programs (CIP) review, and *new customer limited to in-person submission of new account application* are considered most effective relative to other account application processes in mitigating payments fraud. All FI respondents over $1 billion in size use KYC and CIP programs, and 75% state these methods are very effective. Only 45% of the large FIs limit account opening processes to in-person application submissions with slightly over half of those rating it very effective.

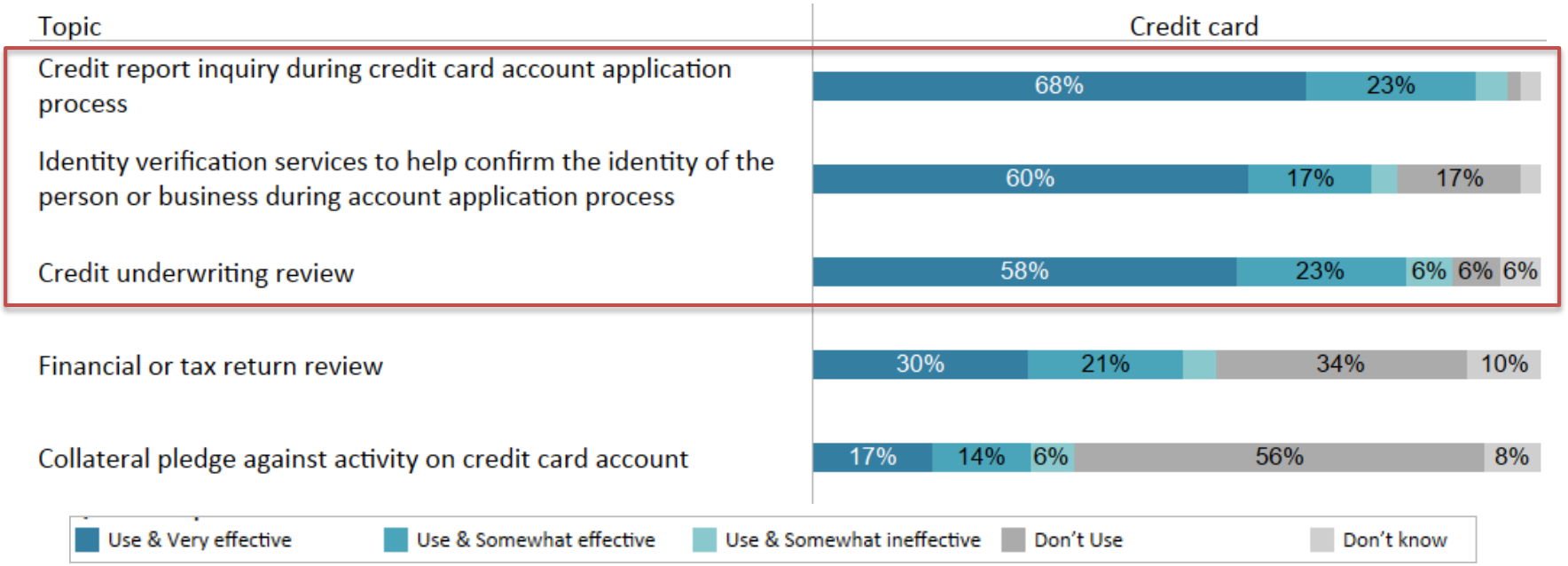
Which account application processes does your financial institution use to mitigate risks when establishing new demand deposit or transaction accounts?



Credit Card Application Fraud Mitigation

Over 80% of FIs use three of the five credit card account application processes (below) with over two-thirds of the FIs rating them as very effective. Note, as shown in the credit card attacks section that follows, application fraud (*fraudulent credentials or other data used to establish new credit card accounts*) is not identified as a top fraud attack.

Which of the following account application processes does your financial institution use to mitigate credit card fraud risks?



FIs that offer credit cards are asked this question.

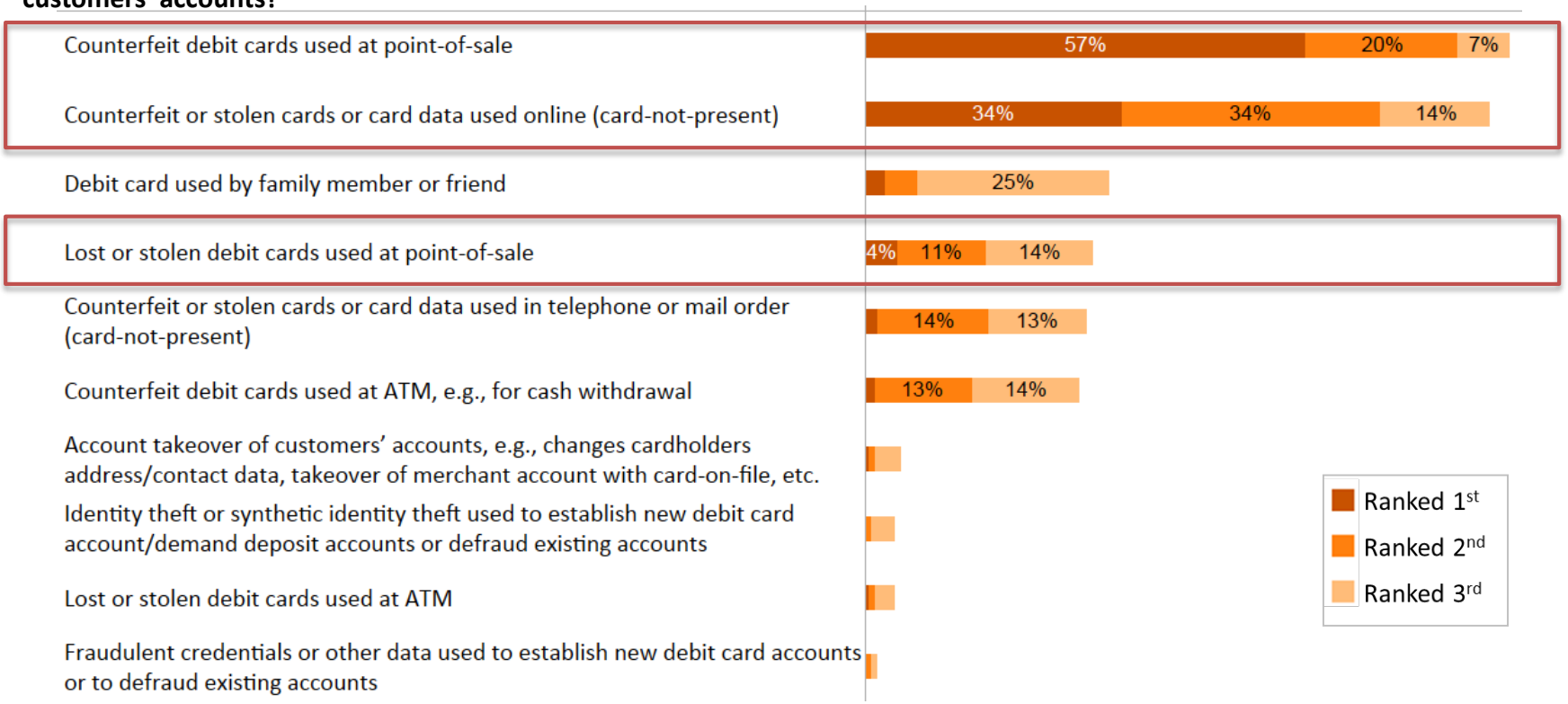
Debit Card Fraud Attacks and Mitigation

Debit Card Fraud Attacks

Eight out of 10 FIs reported *counterfeit debit cards used at point-of-sale* and *fraudulent use of card data online* as the most often used fraud attacks. Combined, these two attacks are ranked as the top debit card attacks by 90% of FIs that offer debit cards.

Lost and stolen card used at point of sale attacks are ranked relatively low, and PIN authentication is generally associated as a primary mitigation method.

What are the three current fraud attacks most often used to initiate debit card fraud against your financial institution or your customers' accounts?



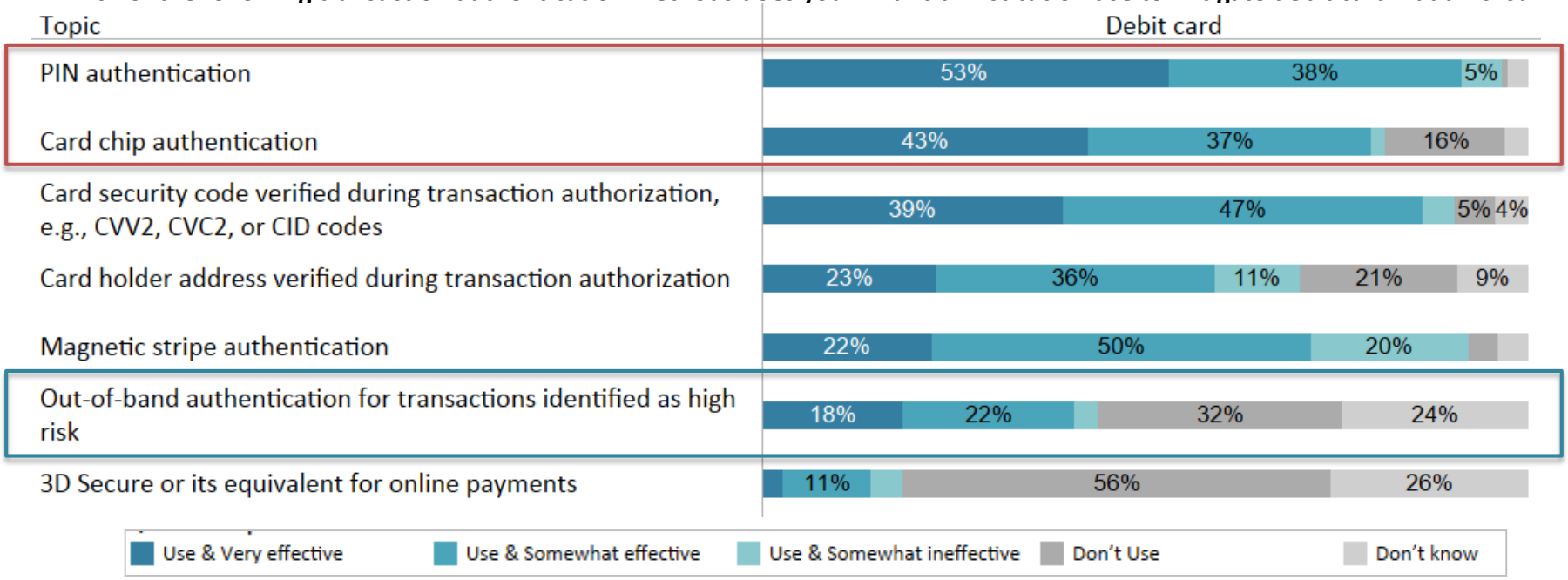
Debit Card Fraud Mitigation - Authentication

For debit cards, *PIN authentication* has the highest adoption rate and effectiveness rating. Eight out of ten FIs report they are issuing *chip cards for authentication* illustrating that the industry is progressing with chip card adoption. Forty-three percent said *chip card authentication* is very effective. While *mag stripe authentication* is widely used, respondents give it a less favorable rating; 20% said it is somewhat ineffective.

Forty-three percent of respondents use *out-of-band authentication for transactions identified as high risk*; however, less than half of those using the method consider it very effective.

About three out of 10 large institutions ($1 billion or more in assets) use *3D secure or its equivalent for online payments*; however, none of them rate this method as very effective and two-thirds of those institutions rated it somewhat ineffective.

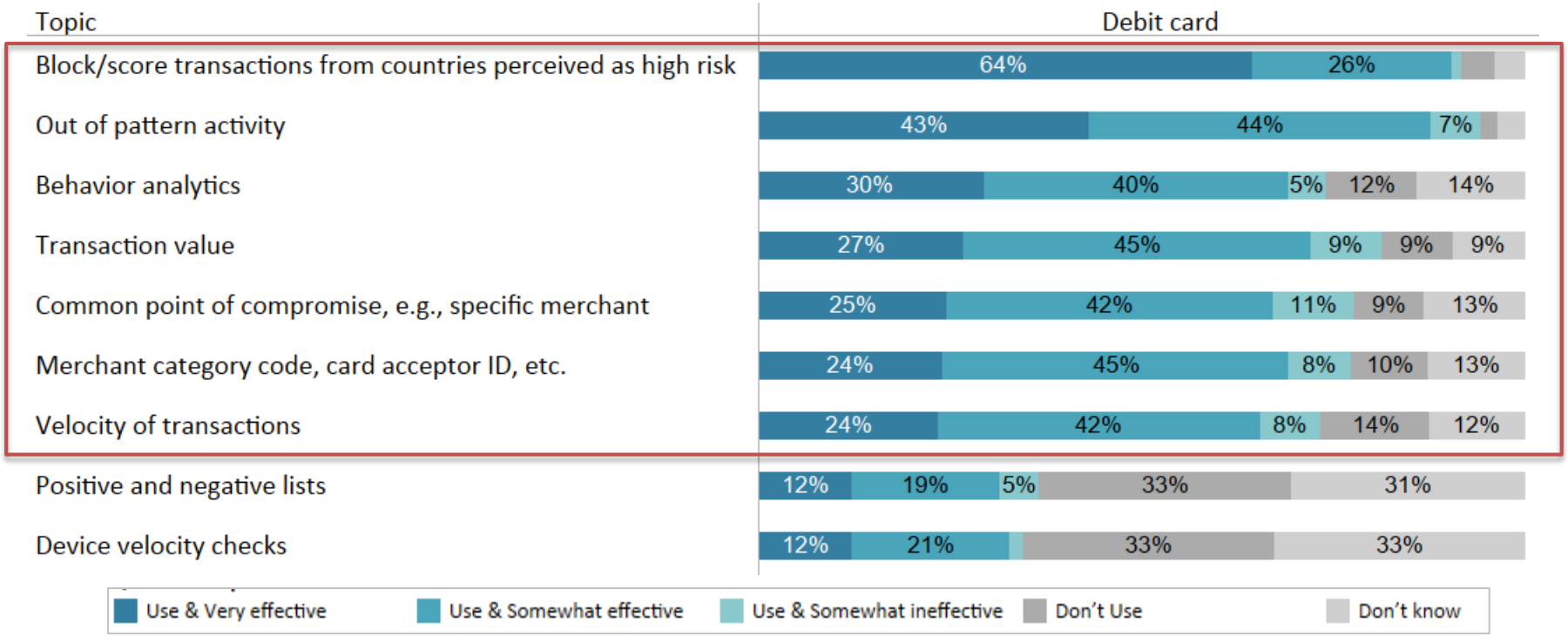
Which of the following transaction authentication methods does your financial institution use to mitigate debit card fraud risks?



Debit Card Fraud Mitigation – Screening/Scoring

It is noteworthy that in the next section the data shows that 65% of respondents outsourced their card fraud management, which may impact the data that they are able to use versus what they would like to use. Seven types of data listed are used by 70% of FIs in their fraud screening tools. This seems to illustrate the need to incorporate many types of data to develop sophisticated fraud detection rules that look at the combination of data factors. Most of the seven types of data are rated moderately effective. *Blocking/scoring transactions from countries perceived as high risk* is rated very effective. *Behavior analytics* and *velocity of transactions* data are used by more of the larger FIs.

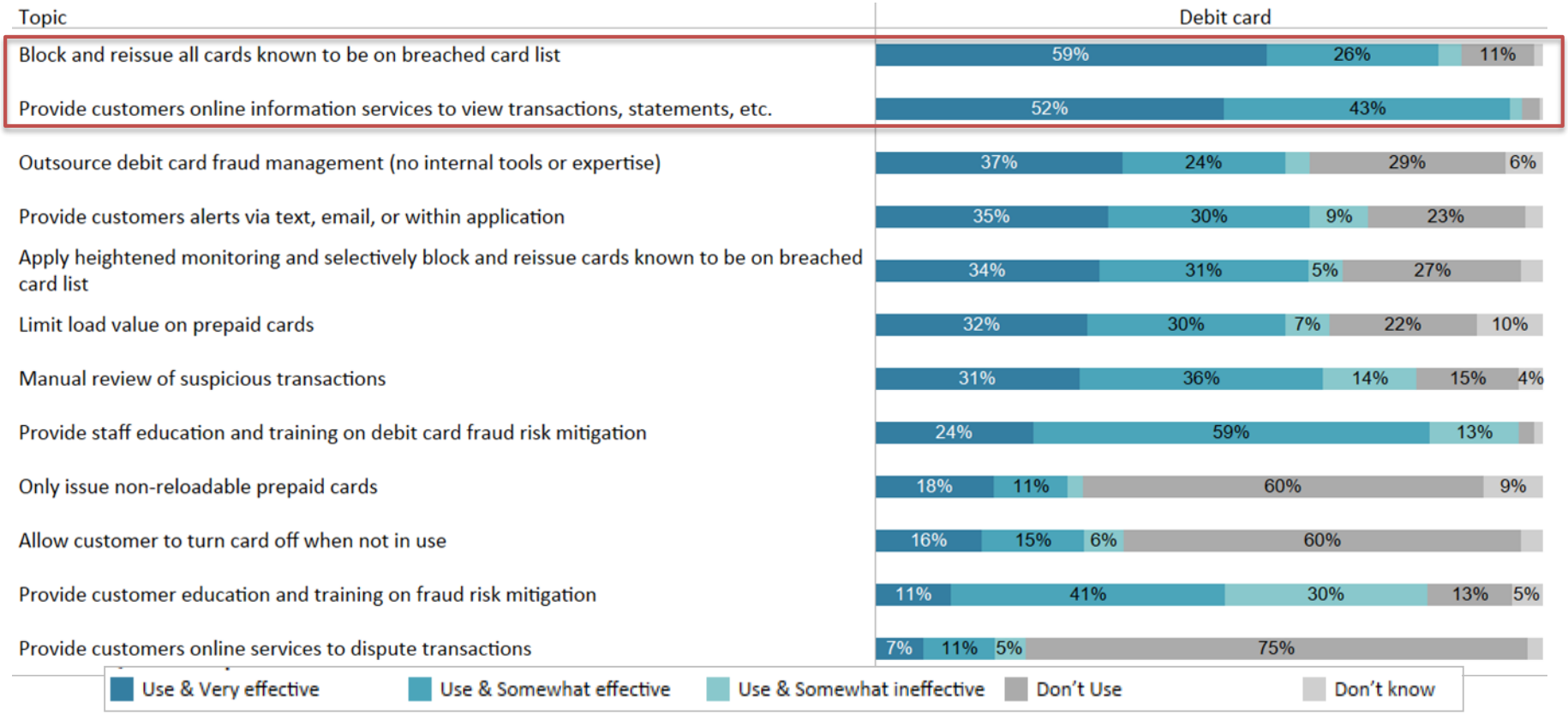
Which of the following data does your financial institution incorporate into fraud screening tools to mitigate debit card fraud risks?



Debit Card Fraud Mitigation – Reporting and Other Risk Management Methods

Blocking and reissuing cards known to be on the breached card list has the highest effectiveness rating and is rated very effective by 59% of respondents. Nearly all FIs *provide customers access to online information service to view transactions and statements*. The effectiveness rating, which is somewhat high, seems to indicate some reliance on customers detecting fraud when other methods did not block the transaction from occurring.

Which of the following reporting and other risk management methods does your financial institution use to mitigate debit card fraud risks?



Credit Card Fraud Attacks and Mitigation

Credit Card Attacks

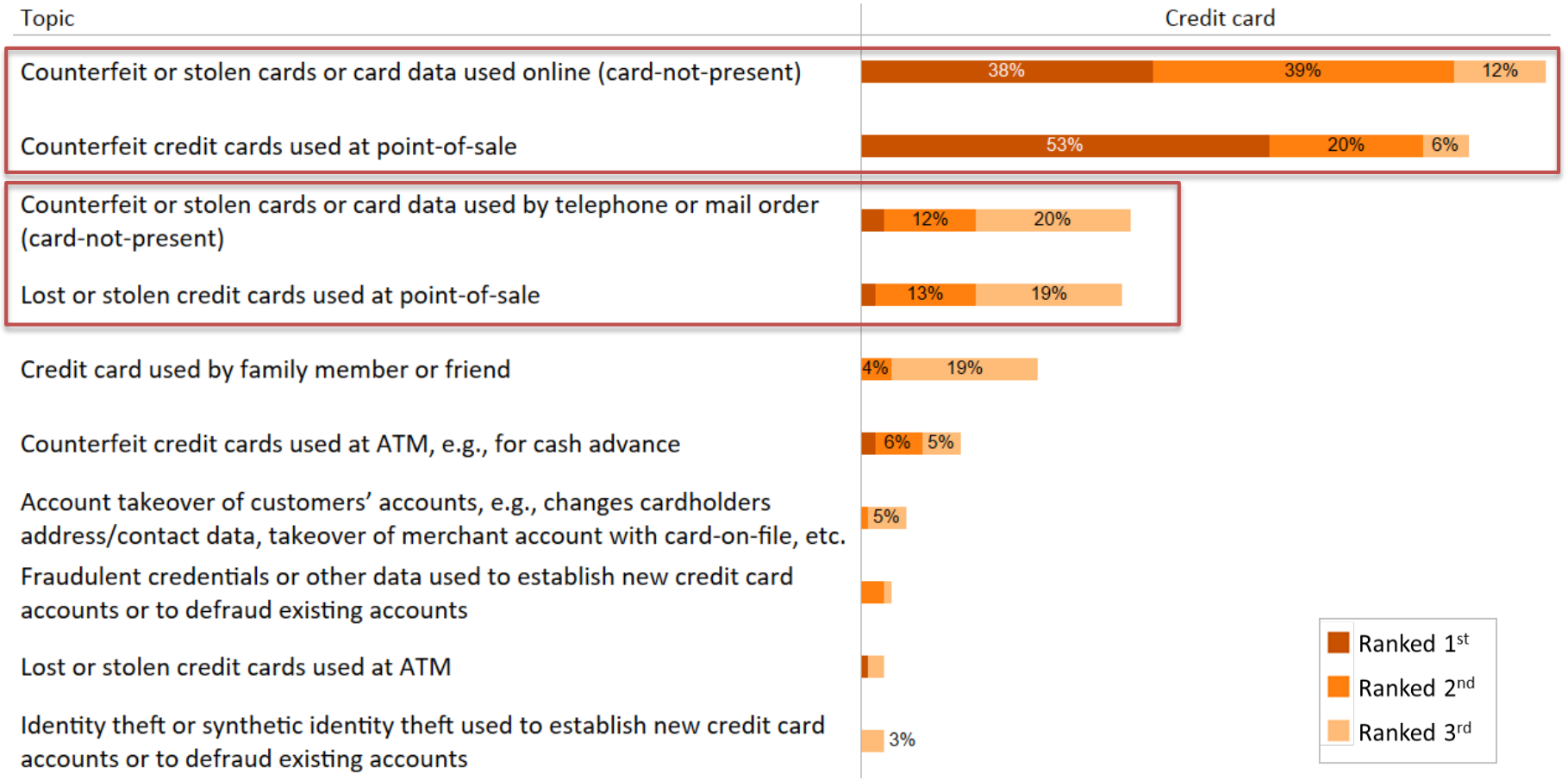
Card-not-present fraud attacks online are in the top three attacks for 89% of FIs that issue credit cards (see chart, page 30). According to the Federal Reserve Payments Study, remote debit and credit card transactions account for 22% of card transactions by number in 2016 and 44% by value. Actual fraud via remote channels accounted for 58.5% of general purpose card fraud (see Federal Reserve Payments Study 2017 Annual Supplement).

Findings in this study confirm online transactions, as a share of card payments, are more likely to be fraudulent. Although 53% of FIs said that attacks using *counterfeit credit cards at point-of-sale* are the most frequent, the ongoing adoption of chip card technology by merchants and FIs may help mitigate this risk. The Federal Reserve Payments Study found that counterfeit card fraud, as a percent of general-purpose card fraud, declined from 43.7% of card fraud value in 2015, to 36% in 2016.

Although *lost and stolen card usage in mail order/telephone order and point-of-sale channels* are ranked in the top three most frequent attacks by some respondents, comparatively the response suggests that lost and stolen card attacks are not as significant (see chart, page 30).

Credit Card Attacks

What are the three current fraud attacks most often used to initiate credit card fraud against your FI or your customers' accounts?

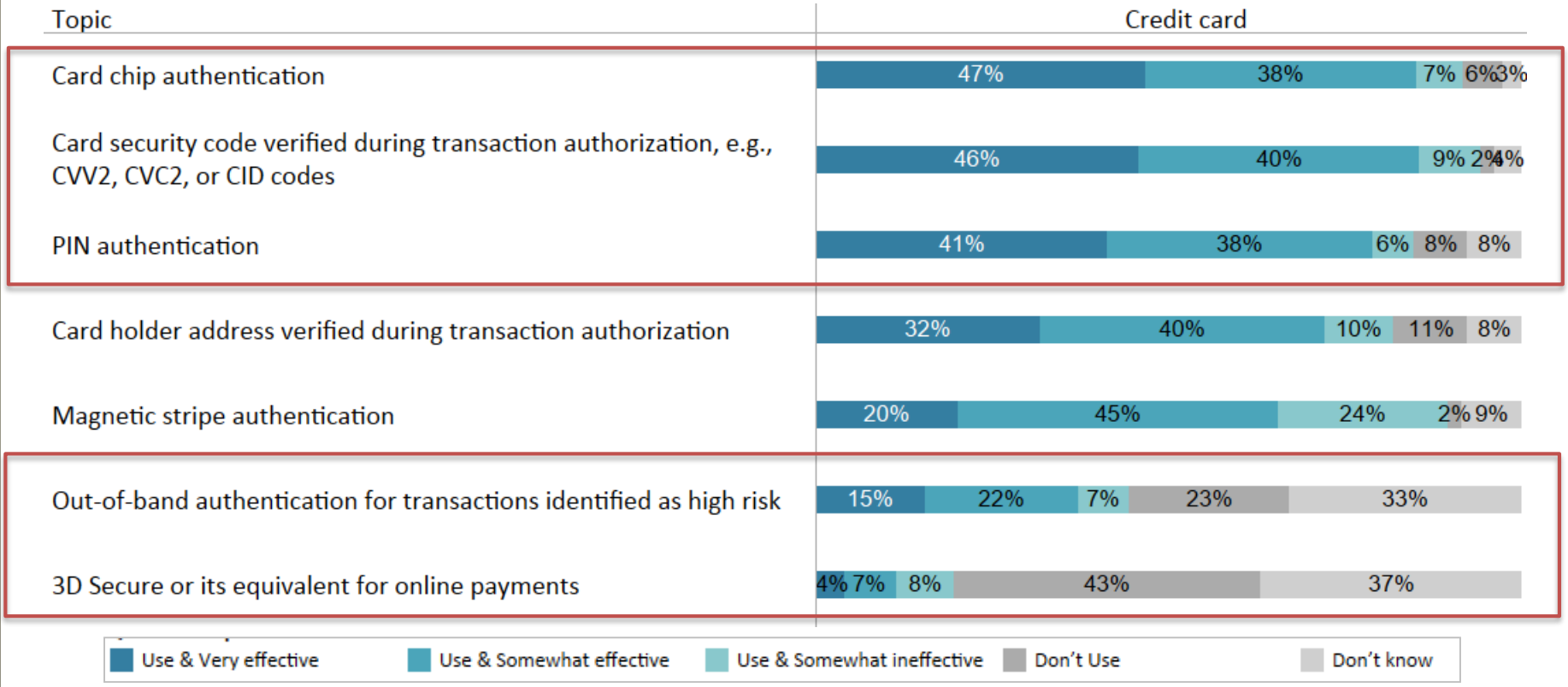


Credit Card Fraud Mitigation – Authentication

Five of the seven authentication methods listed are widely used and usage exceeds 80%. Three of these methods, *security code verification*, *chip card authentication*, and *PIN authentication*, are rated very effective by over 40% of respondents.

Similar to debit cards, 44% of FIs leverage *out-of-band authentication for transactions identified as high risk*, but only one-third of those using it rate it as very effective. Also, *3D secure or its equivalent* received relatively low effectiveness ratings.

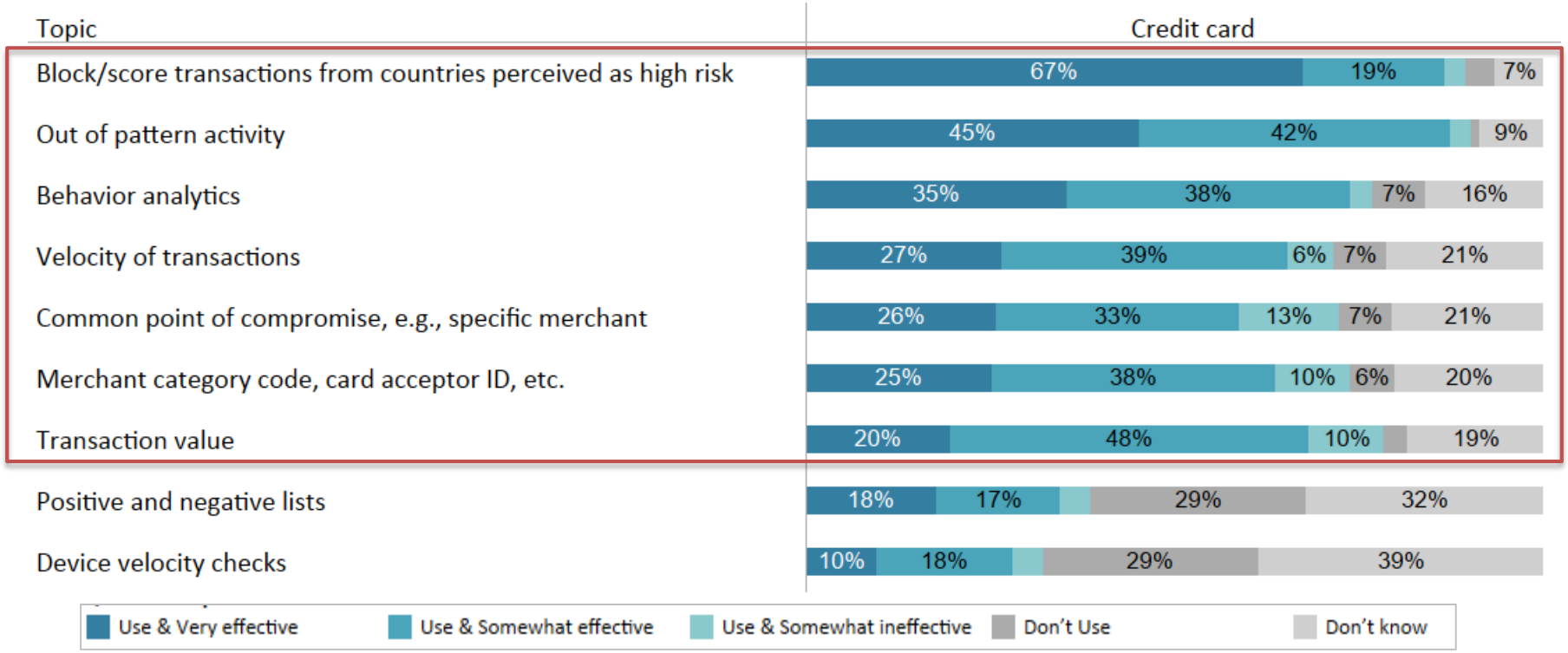
Which of the following transaction authentication methods does your financial institution use to mitigate credit card fraud risks?



Credit Card Fraud Mitigation – Screening/Scoring

Seven of the nine types of data listed are used in fraud screening by 70% or more of the respondents. This is consistent with the debit card findings, and again seems to illustrate the need to incorporate many types of data to develop sophisticated fraud detection rules. *Blocking/scoring transactions from countries perceived as high risk* is the only data type in which two-thirds of respondents indicate high effectiveness. However, this approach may also negatively impact services to customers that travel to those countries.

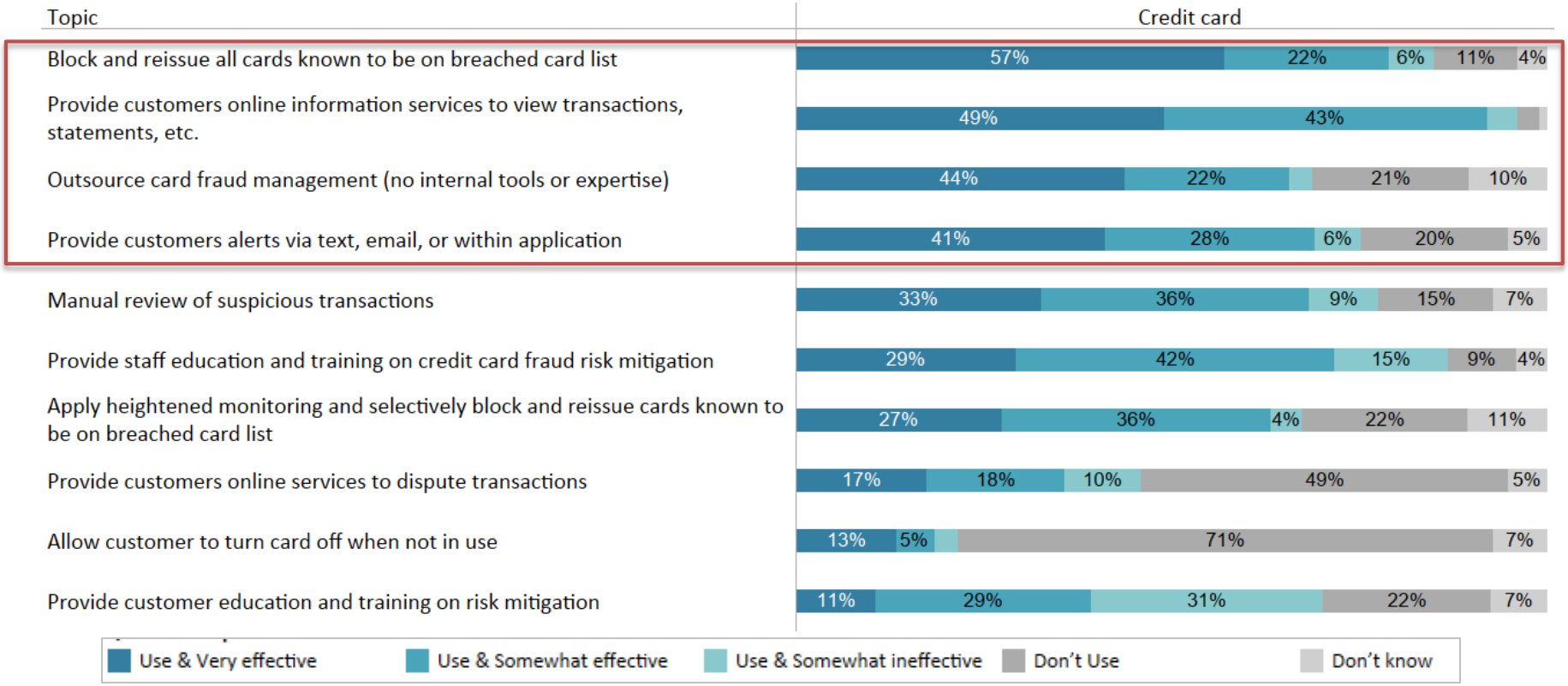
Which of the following data does your financial institution incorporate into fraud screening tools to mitigate credit card fraud risks?



Credit Card Fraud Mitigation – Reporting and Other Risk Management Methods

About two-thirds of the respondents *outsource card fraud management*. *Blocking all cards known to be on the breached card list* is rated very effective by over half of the FIs. It's noteworthy that 92% of FIs offer *customers online information services* and 75% of FIs *provide customer alerts*; both are rated relatively high in terms of effectiveness indicating that FI customers are playing a role in fraud mitigation.

Which of the following reporting and other risk management methods does your financial institution use to mitigate credit card fraud risks?



Check Fraud Attacks and Mitigation

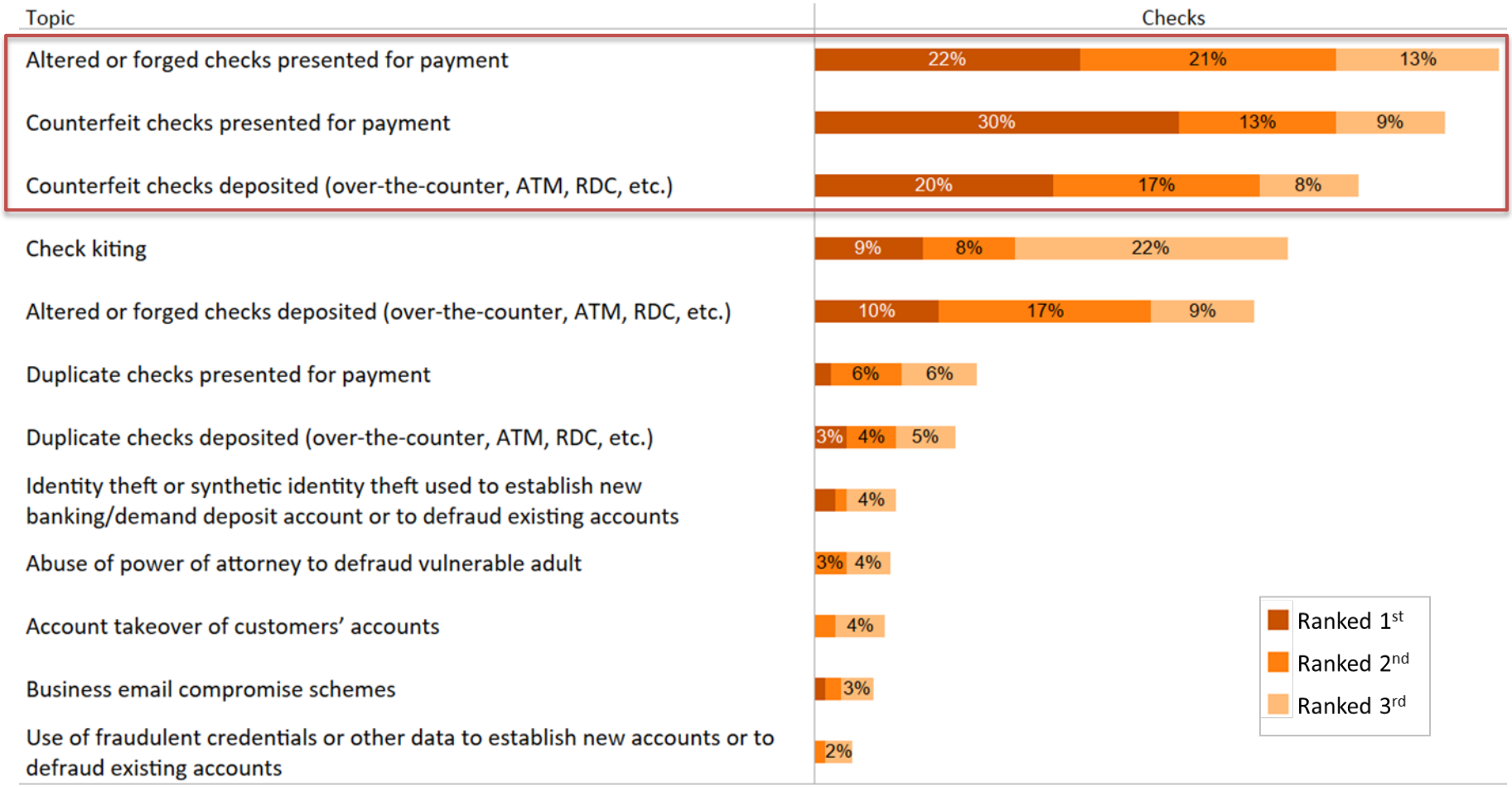
Check Fraud Attacks

There is a greater variety of check fraud attack tactics compared to other payment types. *Altered or forged checks presented for payment*, *counterfeit checks presented for payment*, followed by *counterfeit check deposited* are identified as the most frequent check fraud attacks (see chart page 36).

As discussed earlier, although the number of checks written continue to decline, 66% of respondents state check fraud attempts are in the top three payment types having the highest number of fraud attempts. Twenty-eight percent of respondents report growth in check fraud losses in 2016 compared to 2015.

Check Fraud Attacks

What are the three current fraud attacks most often used to initiate check fraud against your financial institution or your customers' accounts?

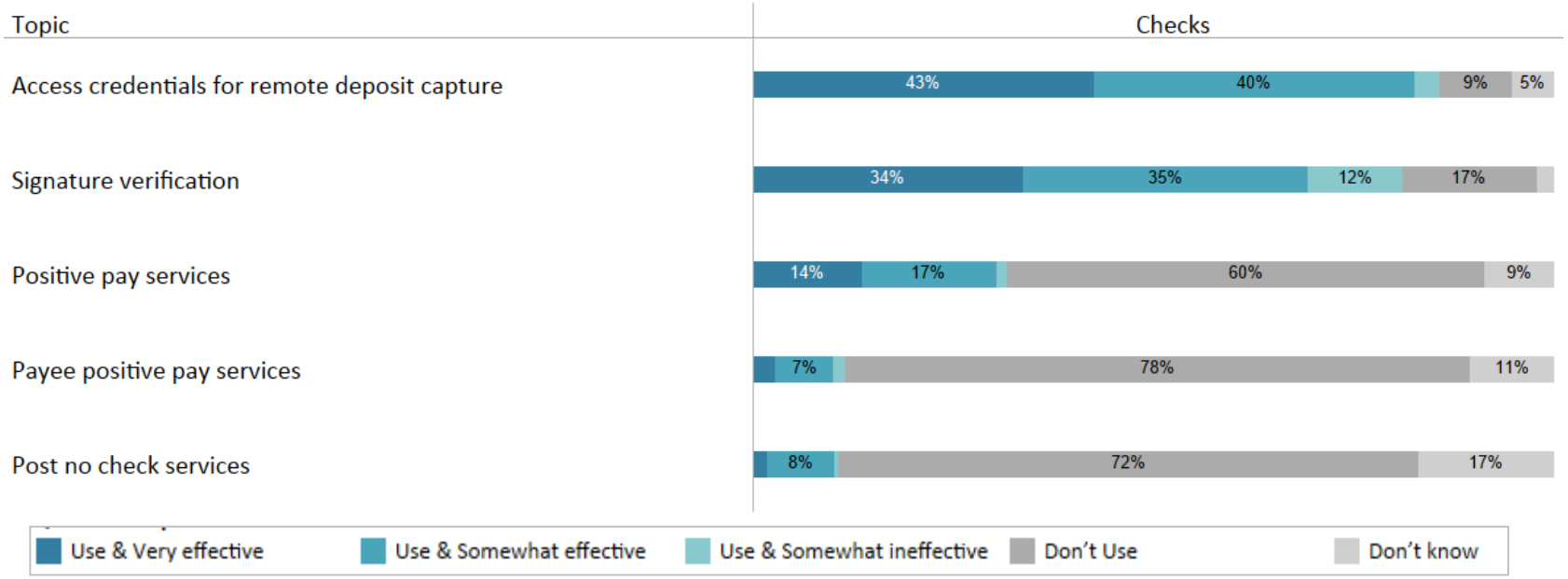


Check Fraud Mitigation – Authentication

There are limited methods for authenticating check payments, which makes it a vulnerable payment method. Eighty-six percent of FIs that offer remote deposit capture (RDC) services use *access credentials* (a verifiable set of data presented by the customer as evidence of identity when accessing RDC services.) Eighty-one percent of FIs complete *signature verifications*.

Positive pay services are used by 31% of respondents. Although this is somewhat low, *positive pay services* are typically geared toward business clients. For FIs whose payment service clients are mostly businesses or a mix of business and consumers, rates of adoption are higher for *positive pay* (45%) and *post no checks* (17%).

Which of the following transaction authentication methods does your financial institution use to mitigate check fraud risks?

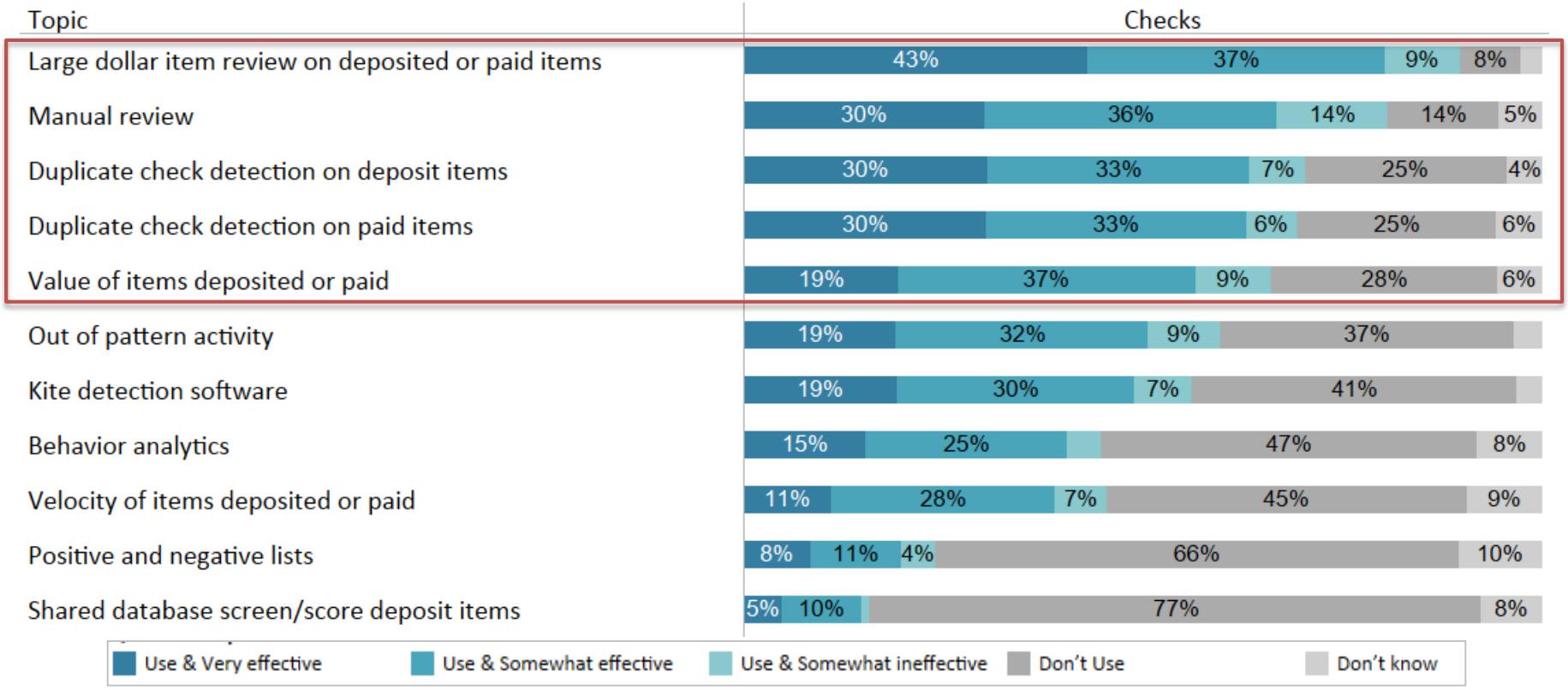


Only FIs that offer remote deposit capture services are asked about access credentials.

Check Fraud Mitigation – Screening/Scoring

Two-thirds of FIs use five of the 11 check fraud screening and scoring methods listed. Of those, only 42% of FIs under $50 million in assets use *duplicate check detection on deposit or paid items* compared to over 70% by FIs in other size categories. *Kite detection software* is used by 56% of respondents; however, only 16% of the FIs under $50 million use this method.

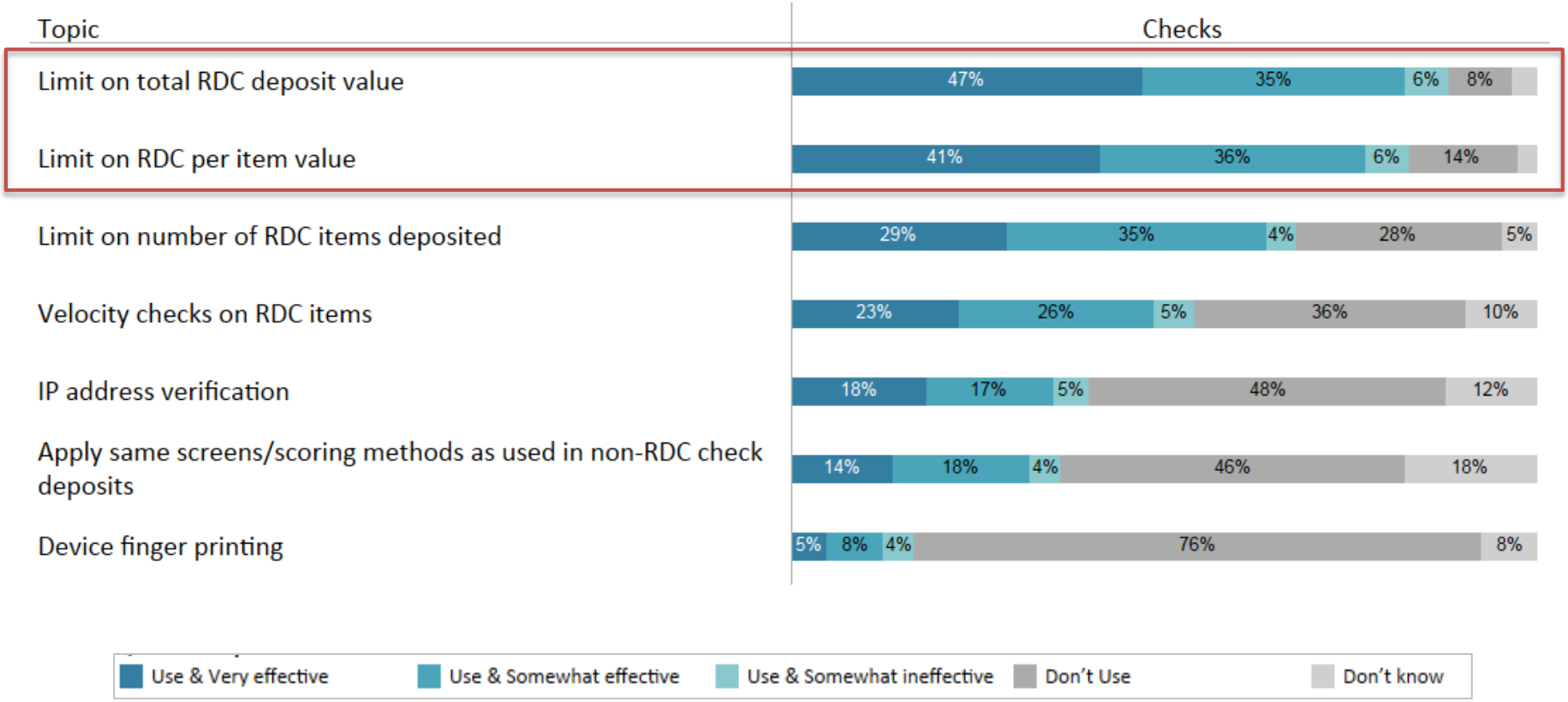
Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate check fraud risks?



Check Fraud Mitigation – Remote Deposit Capture (RDC)

As for fraud screening and scoring methods applied to RDC deposits, *restrictions on deposit value* have the highest usage rates and nearly half of users rate it very effective.

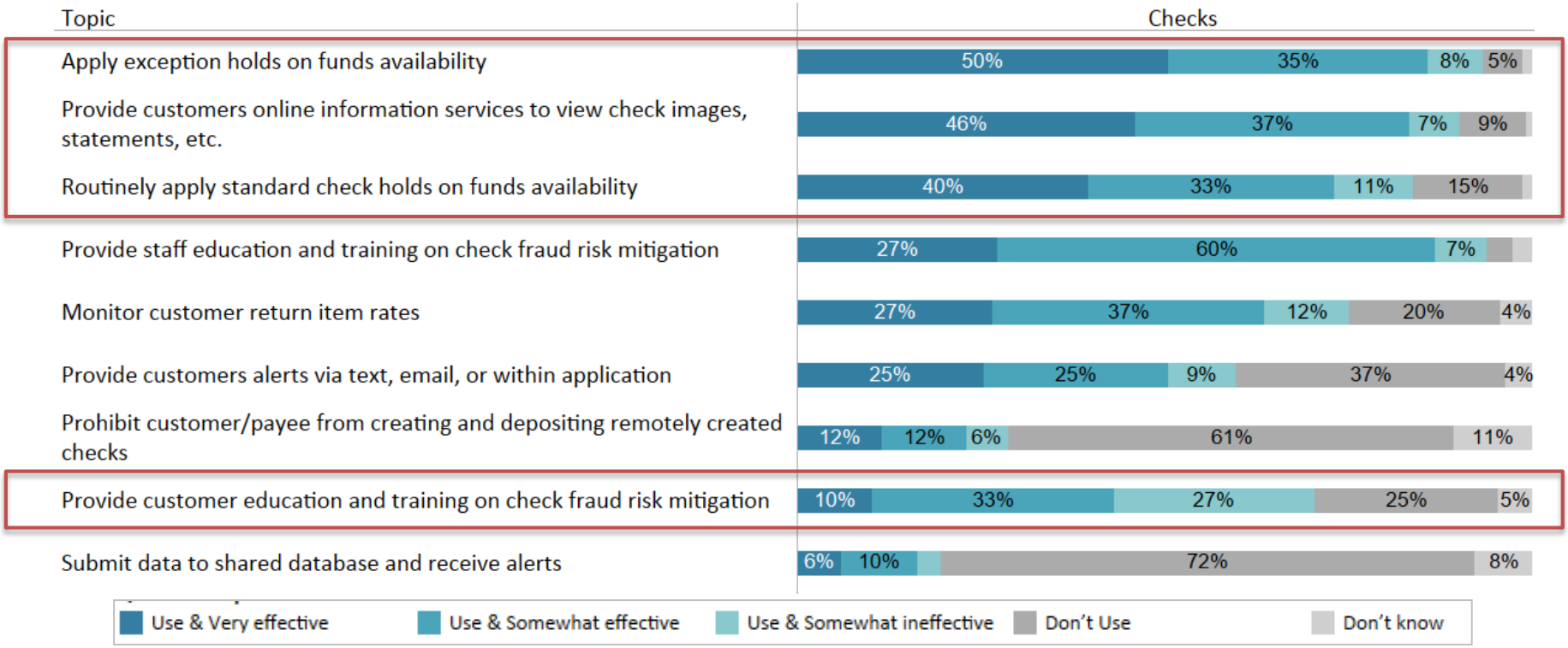
Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate check RDC fraud risks?



Check Fraud Mitigation – Reporting and Other Risk Management Methods

Half of the FIs said *applying exception holds on funds availability* is very effective, and 40% also reported the same for *routinely applying standard check holds*. Nine out of 10 FIs *provide customers online information services*, and rate it effective as a fraud mitigation method. Although customers are playing a role, many FIs that *provide customer education on check fraud* view it as somewhat ineffective.

Which of the following reporting and other risk management methods does your financial institution use to mitigate check fraud risks? For those used, please rate effectiveness.



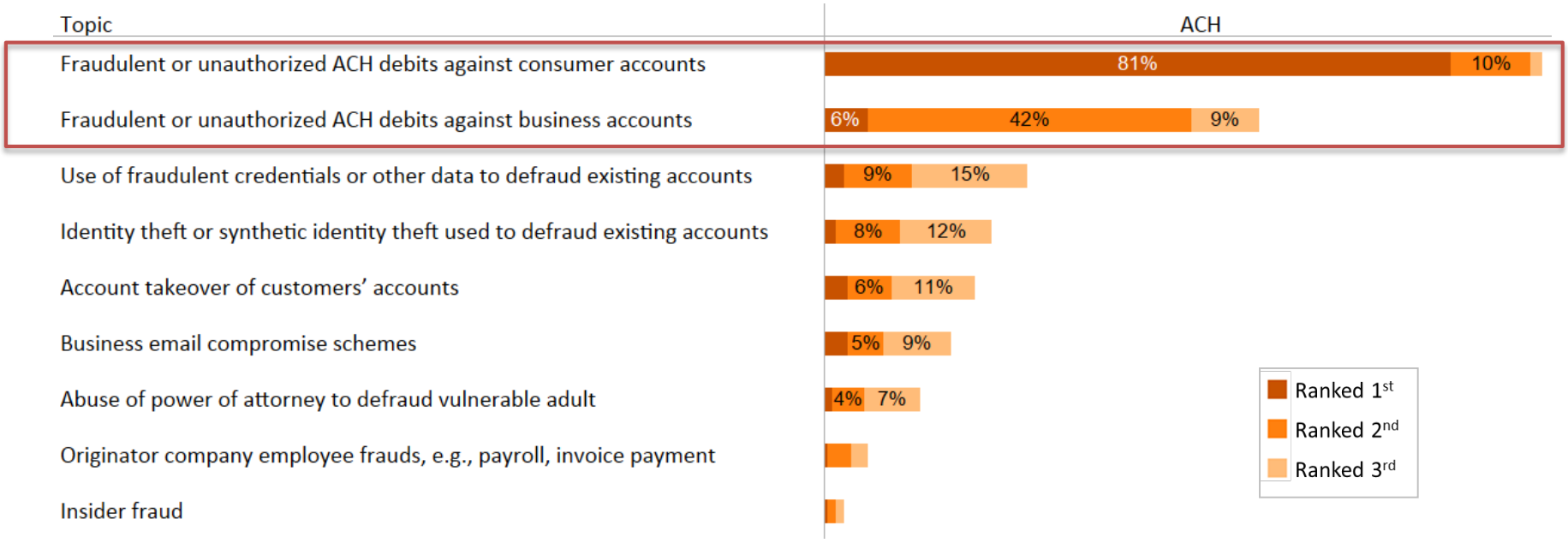
ACH Fraud Attacks and Mitigation

ACH Fraud Attacks

Eight out of 10 FIs that offer ACH services rank *fraudulent or unauthorized debits against consumer accounts* as the number one most frequent attack. *Fraudulent or unauthorized debits against business* accounts is ranked second. Although not all "unauthorized" ACH transactions are fraudulent, the responses are provided in the context of fraud attacks.

For FIs whose payment service clients are mostly businesses or a mix of business and consumers, the top two attacks do not change. However, for these FIs, nearly a third (31%) ranked *business email compromise* attacks in the top three attacks with 6% ranking it first, 7% ranking it second and 18% ranking it third.

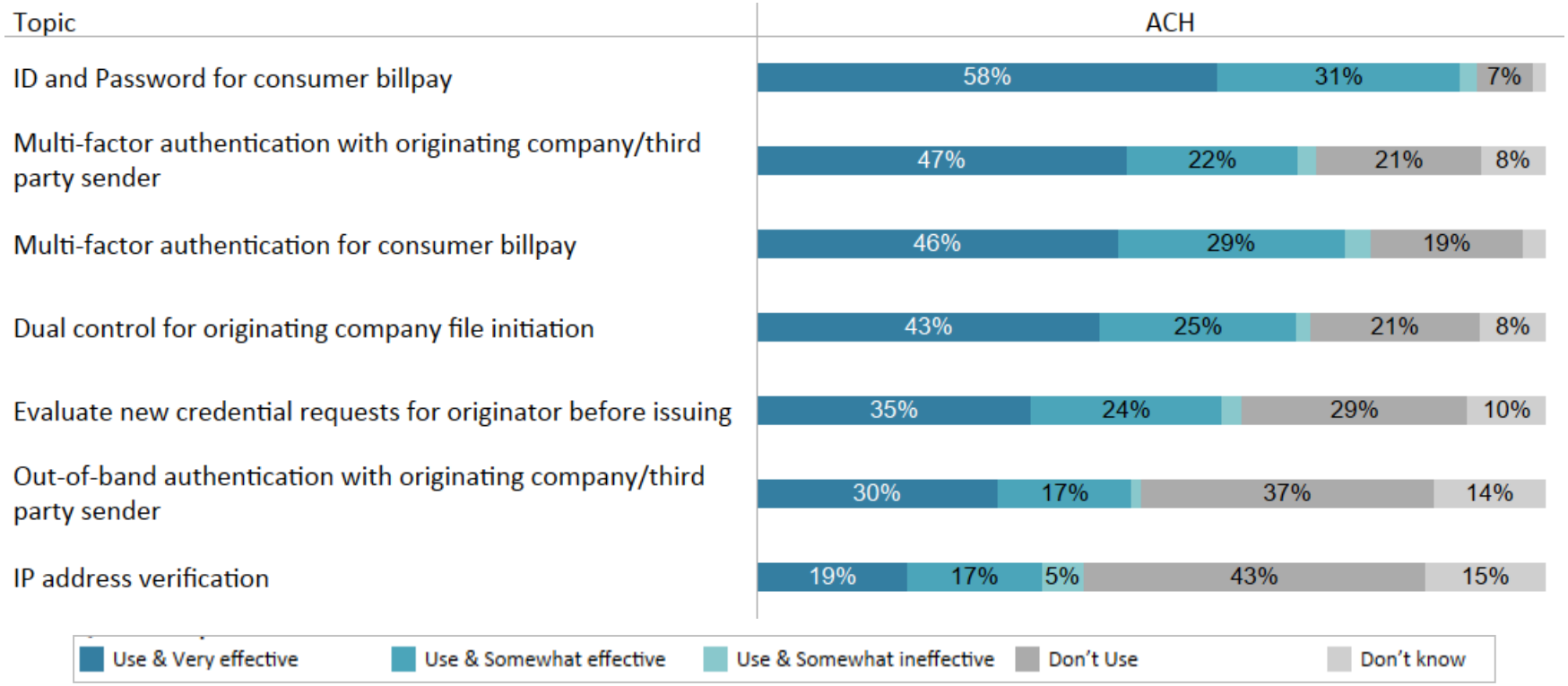
What are the three current fraud attacks most often used to initiate ACH fraud against your financial institution or your customers' accounts?



ACH Fraud Mitigation – Authentication

FIs that offer billpay or ACH origination services are asked what methods they use for authentication. With one exception (IP address verification), all of the authentication methods are ranked very effective by over half (55% to 67%) of the FIs that use them. This seems to indicate relatively high satisfaction in these methods.

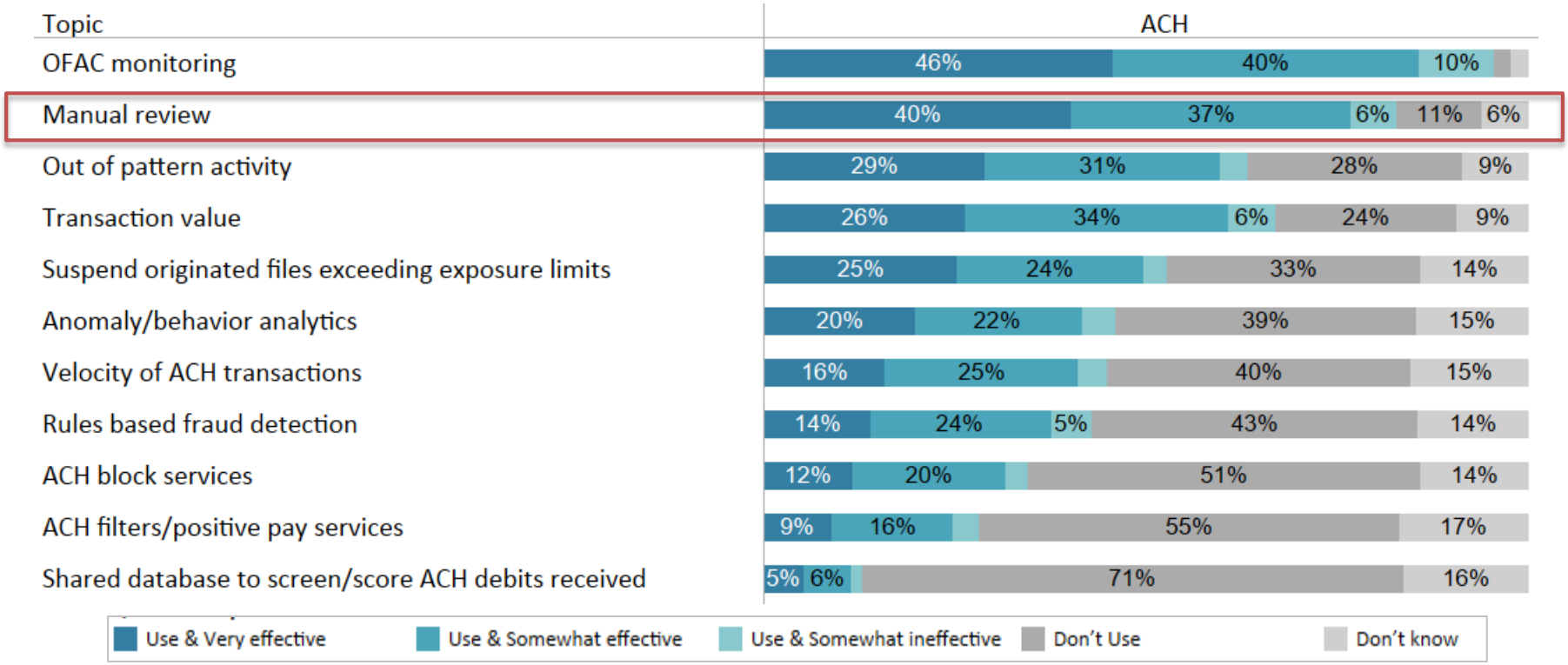
Which of the following ACH originator/sender authentication methods does your financial institution use to mitigate ACH fraud risks?



ACH Fraud Mitigation – Screening/Scoring

Manual review processes are used by over 80% of FIs that offer ACH payment services. Nearly half the FIs using *manual review* process rate it as very effective. More than 90% of FIs over $1 billion in size offer both ACH origination and receipt services tend to use more of the screening tools, which may help to identify relative effectiveness of these tools as shown on the next page.

Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate ACH fraud risks?

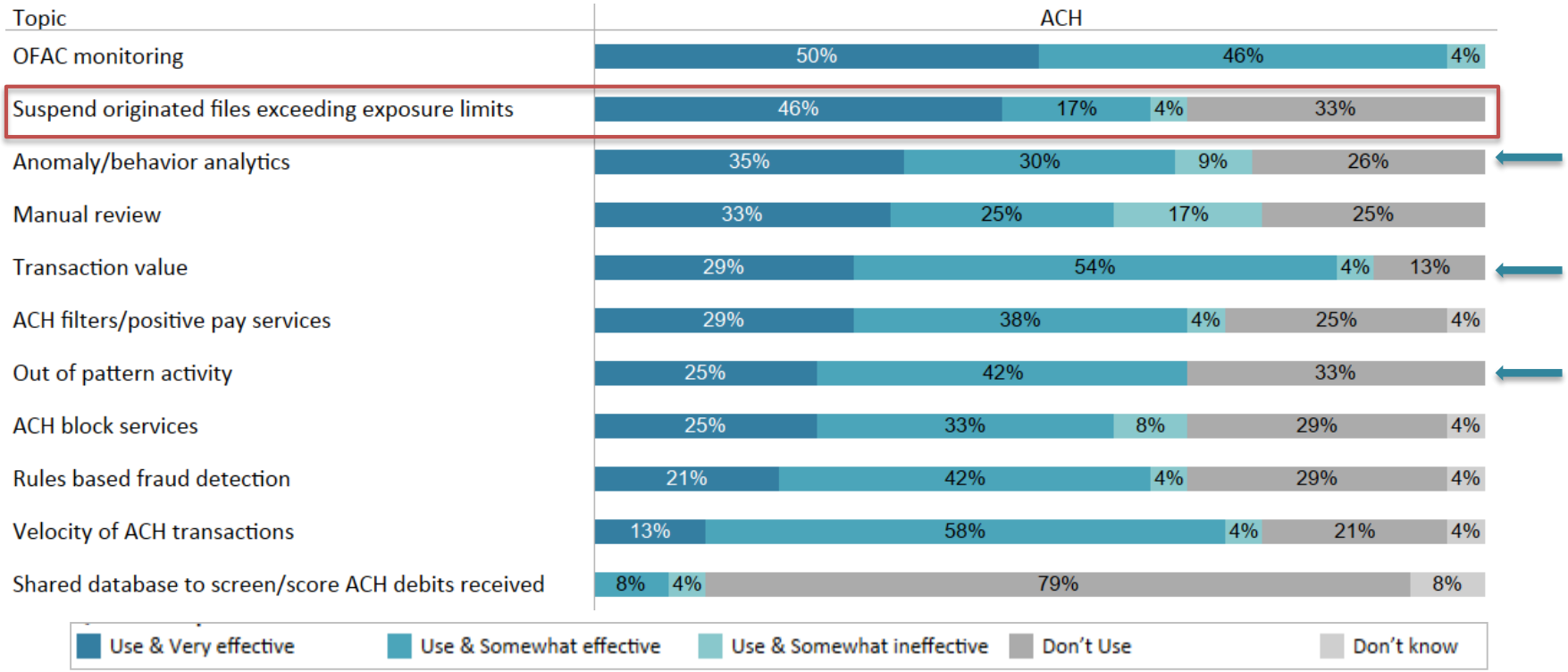


ACH Fraud Mitigation – Screening/Scoring by Respondents $1 Billion and Over in Size

More than 90% of the large FIs offer both ACH origination and receipt services. Their use and effectiveness ratings of ACH screening/scoring tools differs from the "all" respondents average on the last page. This slice of the data provides another view of relative effectiveness. *Manual review* dropped in effectiveness relative to other more automated tools—*anomaly/behavior analytics*, *transaction value*, and *out-of-pattern activity* screening. For methods specific to ACH origination, *suspending originated files exceeding exposure limits* has the highest effectiveness rating with 68% of those using it rating it very effective.

Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate ACH fraud risks?

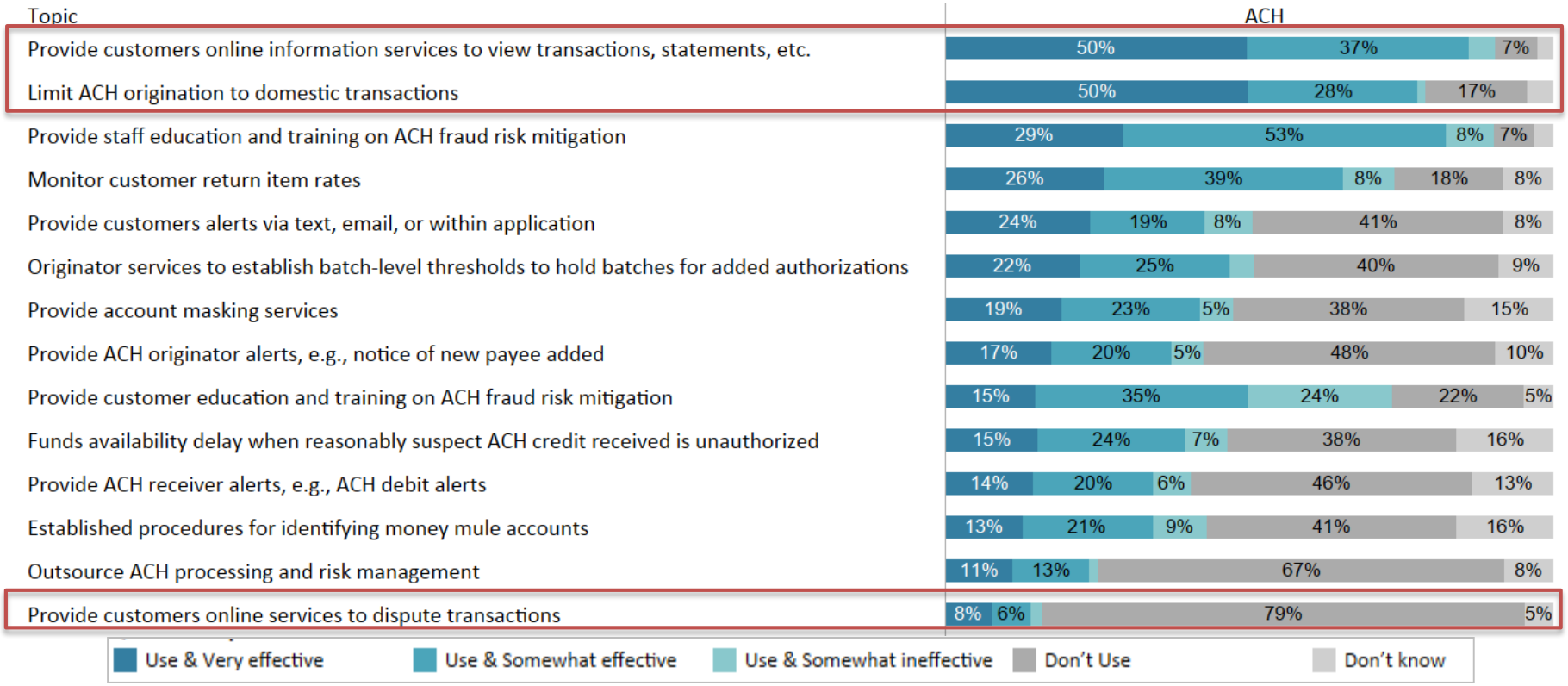
Responses by FIs $1 Billion or More in Assets



ACH Fraud Mitigation – Reporting and Other Risk Management Methods

There are three reporting and other risk management methods listed where 50% or more of the respondents that use the method rank it as very effective. Two of these methods (*provide online information services allowing customers to view transactions and statements* and *provide customers online services to dispute transactions*) rely on customer involvement in identifying fraudulent transactions. The third is *limit ACH origination to domestic transactions*.

Which of the following reporting and other risk management methods does your financial institution use to mitigate ACH fraud risks?

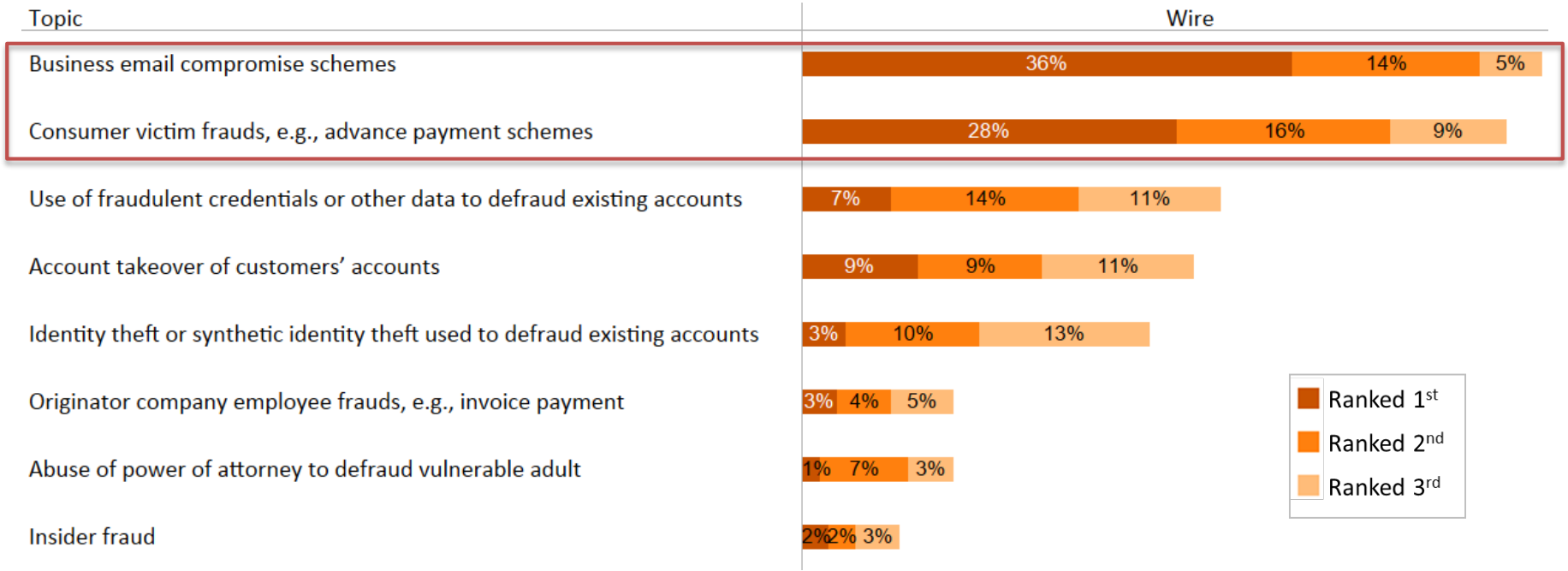


Wire Fraud Attacks and Mitigation

Wire Fraud Attacks

Business email compromise (BEC) attacks and *consumer victim frauds* are identified as the most frequent wire fraud attacks. For the largest FIs (over $1 billion in assets) 74% ranked *BEC* attacks number one and 91% indicated it is in the top three. In contrast, for small FIs (under $50 million), none of the respondents ranked *BEC* attacks first or second and only 5% ranked them third as the most frequent attack. Given that the small FIs are mostly credit union respondents, this is not surprising since their primary customer base is consumers. In slicing the data by FIs' predominant users of payment services, those that are consumer focused ranked *consumer victim frauds* highest with 38% of those respondents ranking it number one and a total of 54% ranking it in the top three.

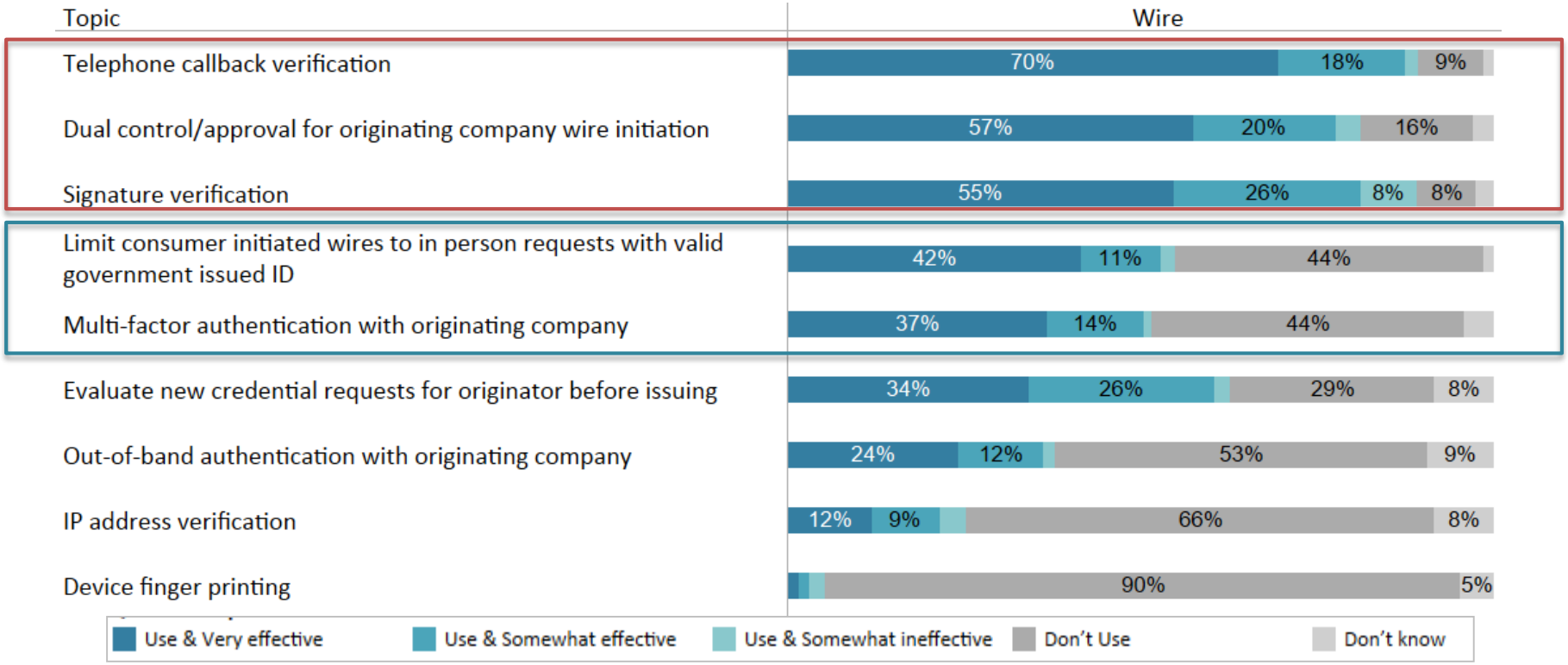
What are the three current fraud attacks most often used to initiate wire fraud against your financial institution or your customers' accounts?



Wire Fraud Mitigation – Authentication

Three of the authentication methods (*telephone callback verification*, *dual control/approval by originating company*, and *signature verification*) are used by over 80% of FIs, and over all, these are rated as very effective. Although adoption is somewhat lower on *limiting consumer wires to in-person request with a valid government ID* and *multifactor authentication with originating company*, these methods are rated high in terms of effectiveness. Given the top attacks—*BEC* and *consumer victim frauds*, these lesser used authentication methods (*limit consumer initiated wires to in-person requests with valid ID* and *multi-factor authentication with originating company*) might help curb these attacks.

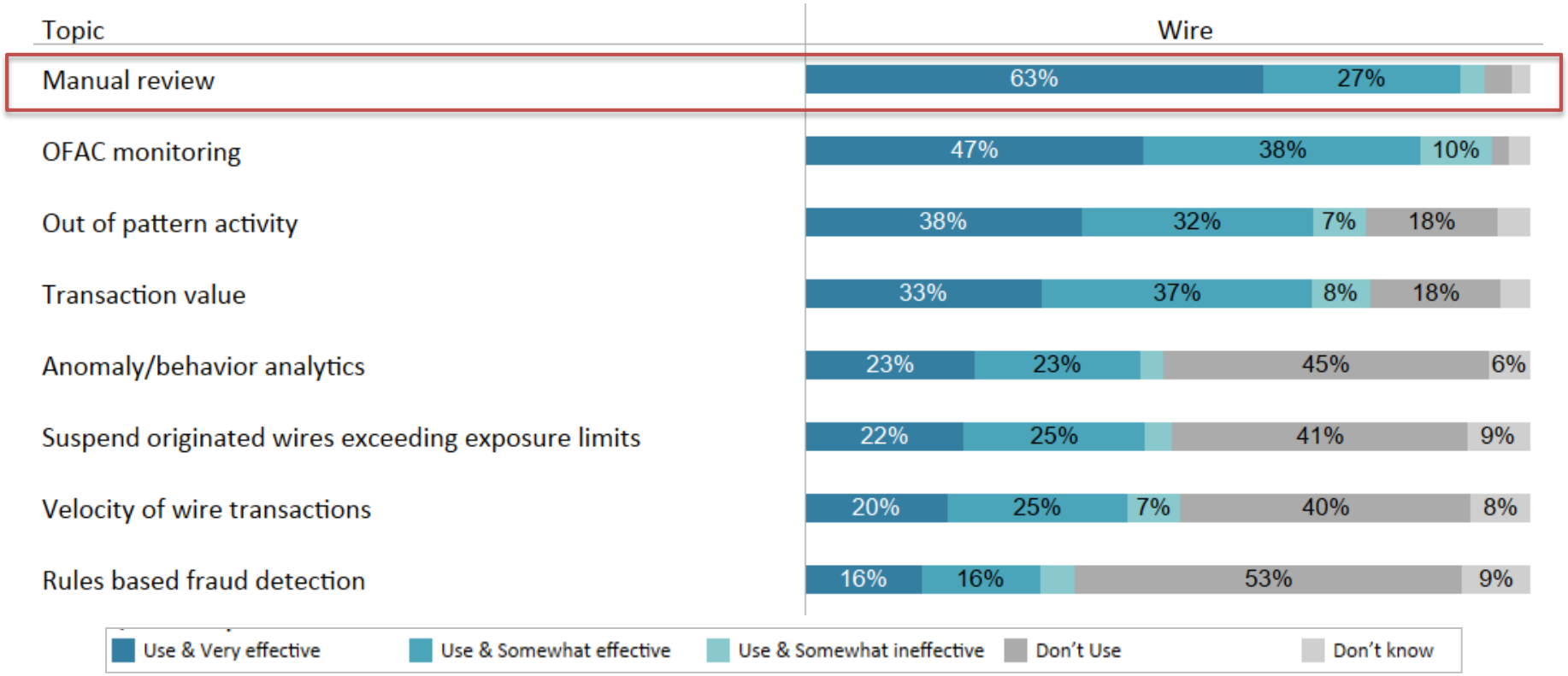
Which of the following transaction authentication methods does your financial institution use to mitigate wire fraud risks?



Wire Fraud Mitigation – Screening/Scoring

Regardless of size, nine out of 10 FIs use *manual review* processes for wire. Although the effectiveness rating of *manual review* is rated very high overall, the rating varied by size of FI with 71% of the smallest FIs (those under $50 million in assets) rating it very effective, compared to 48% of the largest FIs.

Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate wire fraud risks?



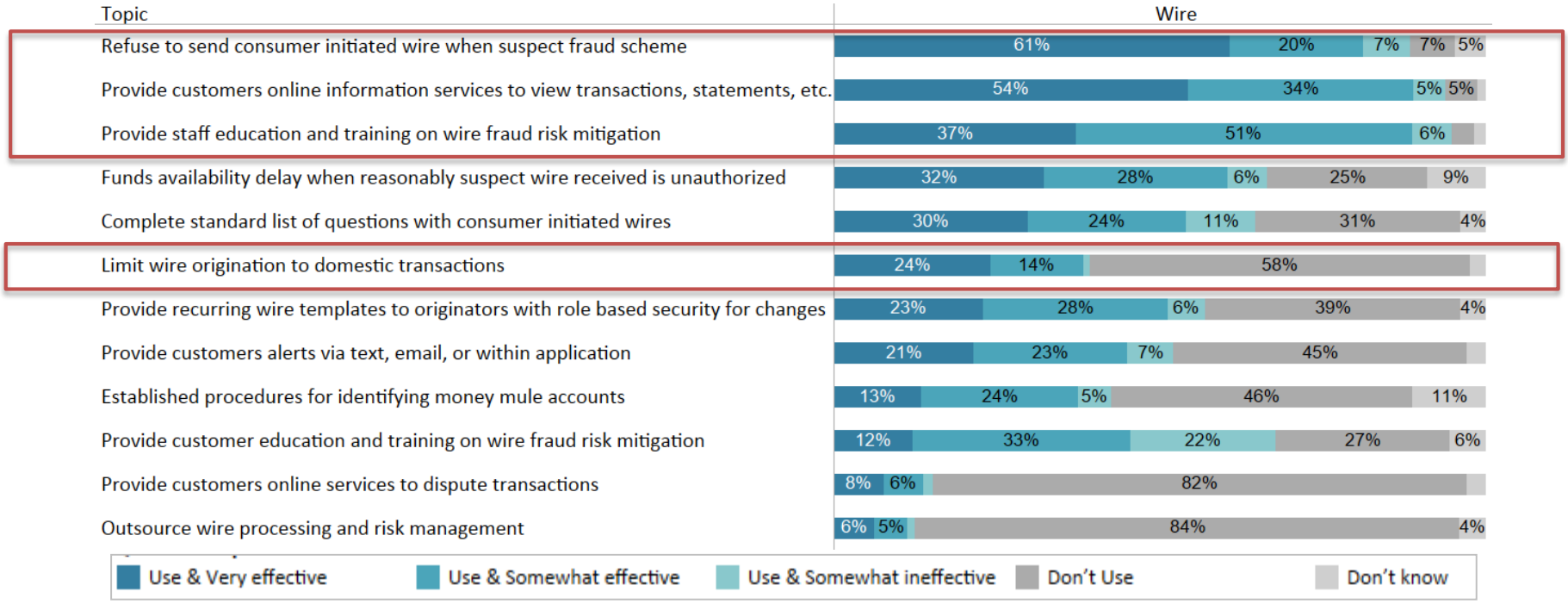
Wire Fraud Mitigation – Reporting and Other Risk Management Methods

Three of the reporting and other risk management methods listed are used by over 85% of respondents. Although *consumer victim frauds* are a concern, 7% of respondents that offer wire transfer services won't *refuse to send a consumer-initiated wire when the FI suspects a fraud scheme*.

Regardless of the FI size, over half of the respondents rank *customer online information services* as very effective. Fed researchers are surprised by this rating given the speed and finality of wire transfers. Once a wire is sent it is very difficult to recover funds.

Similar to ACH, *limit wires to domestic transactions* has a high effectiveness rating by 60% of those that use it.

Which of the following reporting and other risk management methods does your financial institution use to mitigate wire fraud risks?

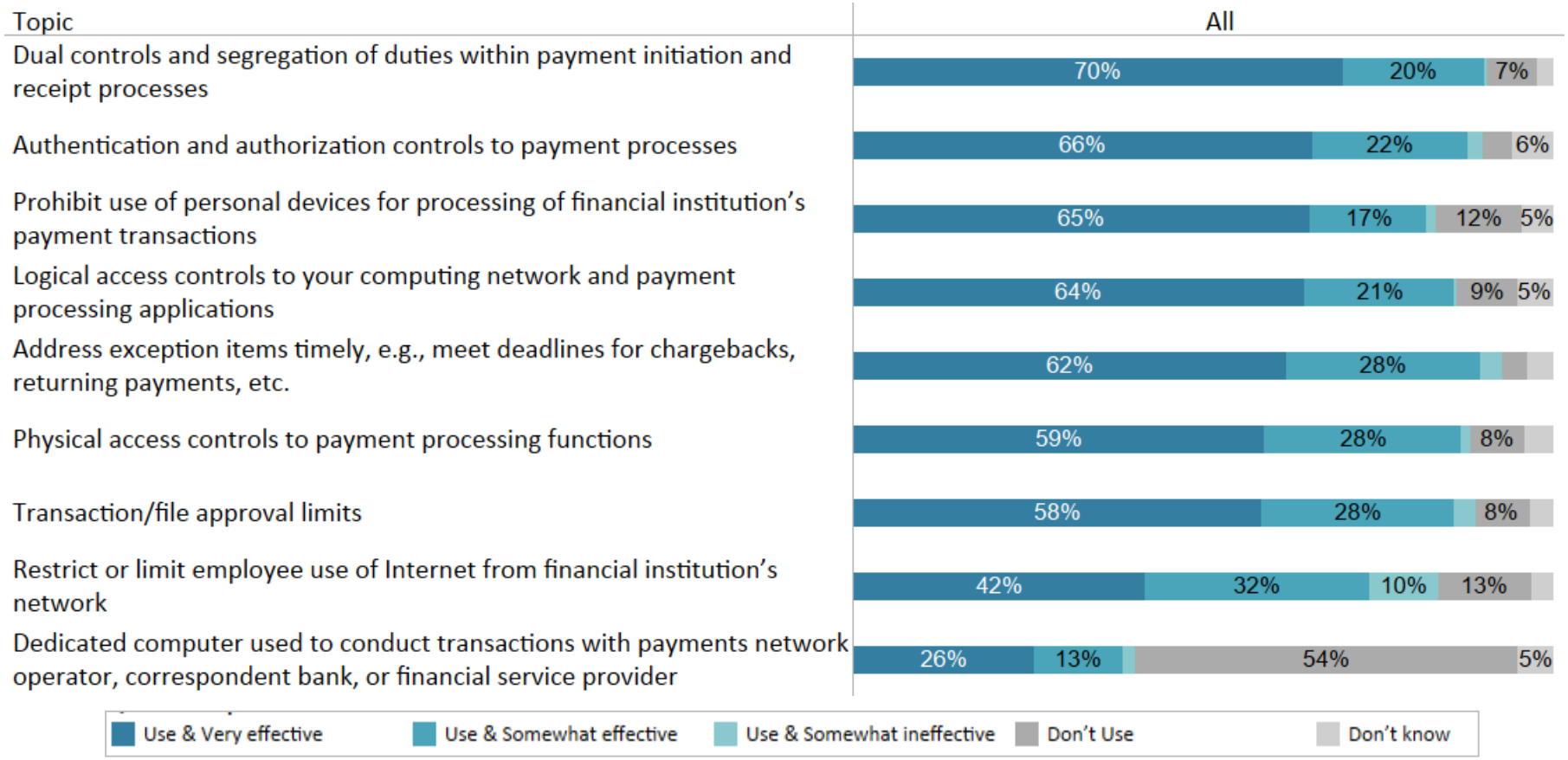


Fraud Mitigation Internal Controls

Internal Controls and Procedures

FIs are avid users of internal controls and procedures that can help reduce payments fraud risks. Eight of the nine internal controls and procedures listed are used by over 80% of the FIs responding to the survey, and nearly all of them are rated very effective by over half of the respondents.

Which of the following internal controls and procedures does your financial institution currently use to mitigate fraud risks?

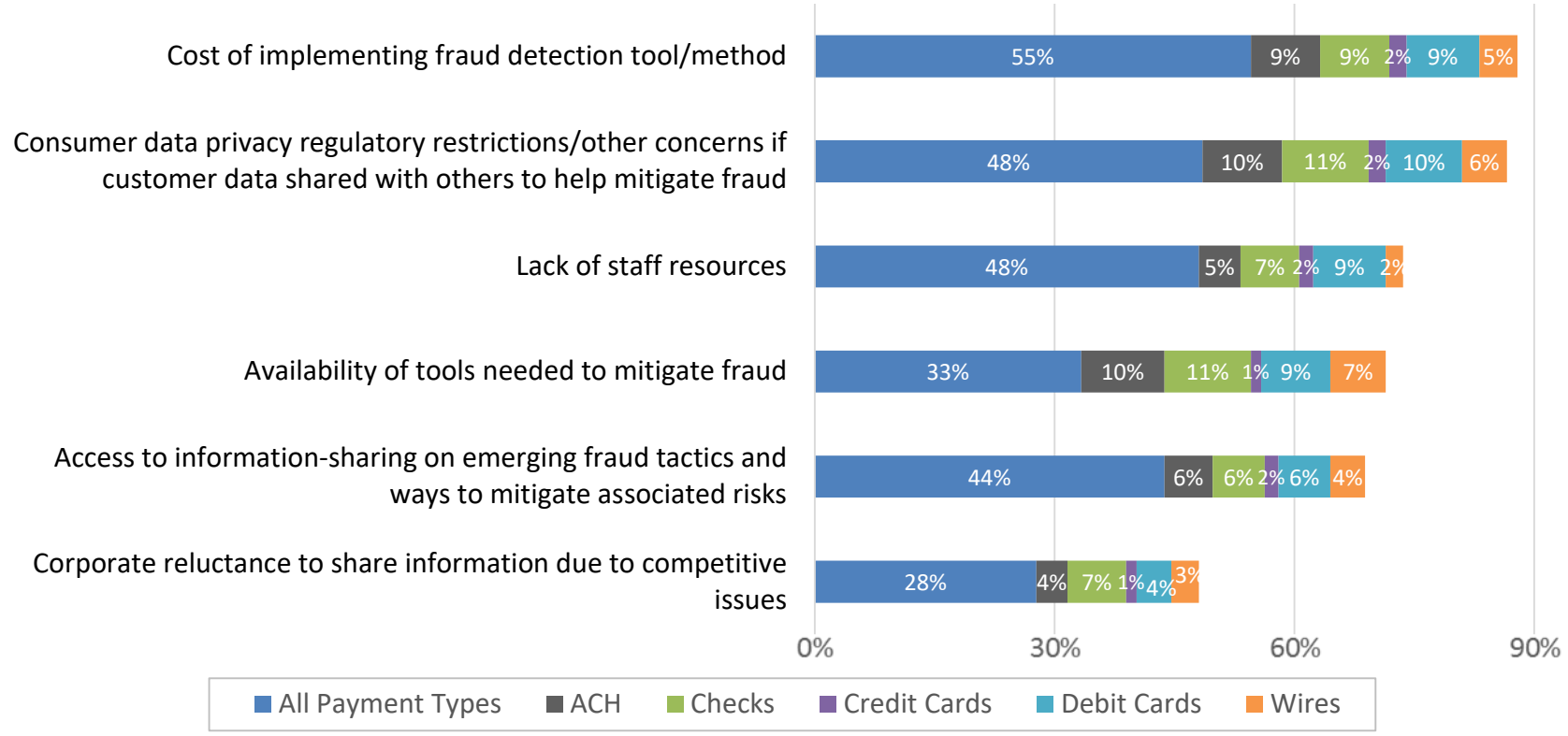


Barriers and Opportunities

Barriers to Fraud Mitigation

Cost of implementing fraud detection tools/methods is considered the largest barrier. *Lack of staff resources*, *access to information-sharing on emerging fraud tactics and ways to mitigate associated risk*, and *concerns about consumer data privacy* are also seen as significant barriers across all payment types.

What are the main barriers to mitigate payments fraud that your financial institution experiences? (Choose all that apply)

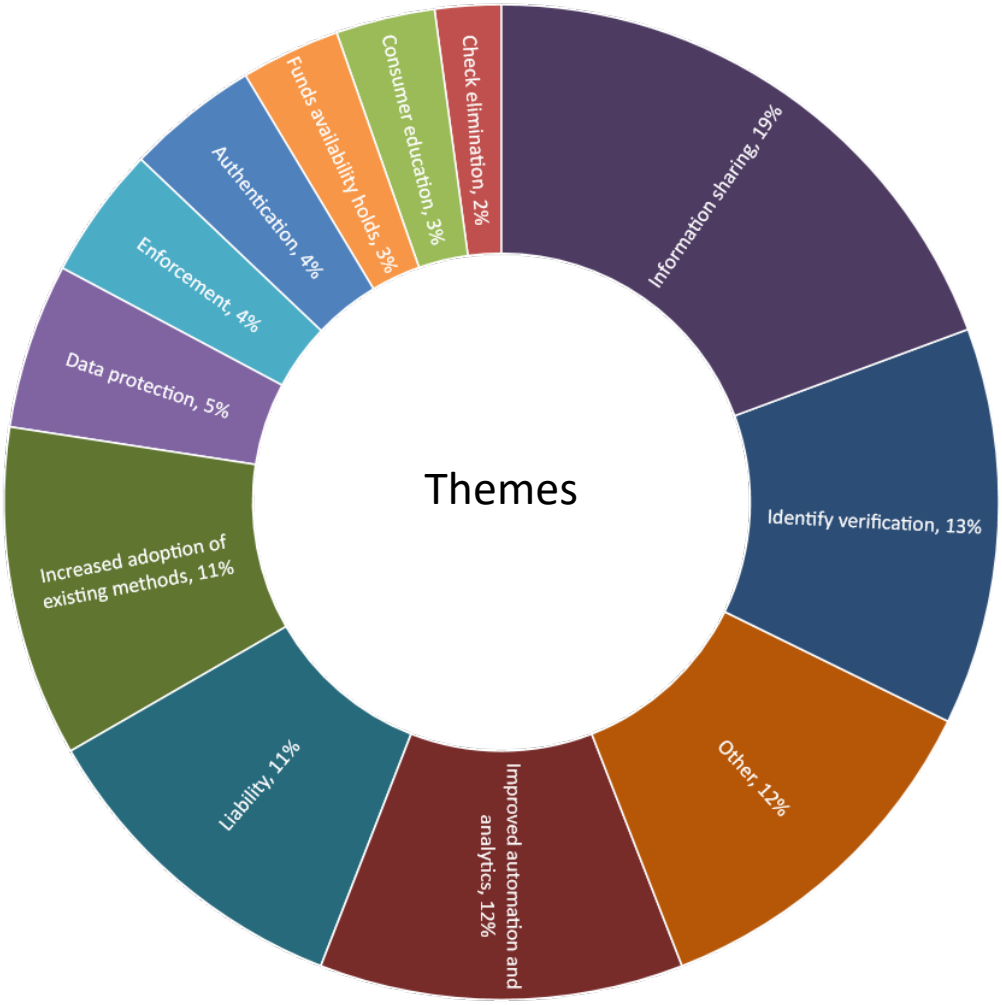


New or Improved Methods Needed

Respondents are asked an open-ended question on what new and improved methods are needed to help mitigate payments fraud. Ninety-three suggestions are offered. Eleven themes emerged as illustrated in the color wheel on the right.

Five themes stood out. Examples of ideas are listed below:

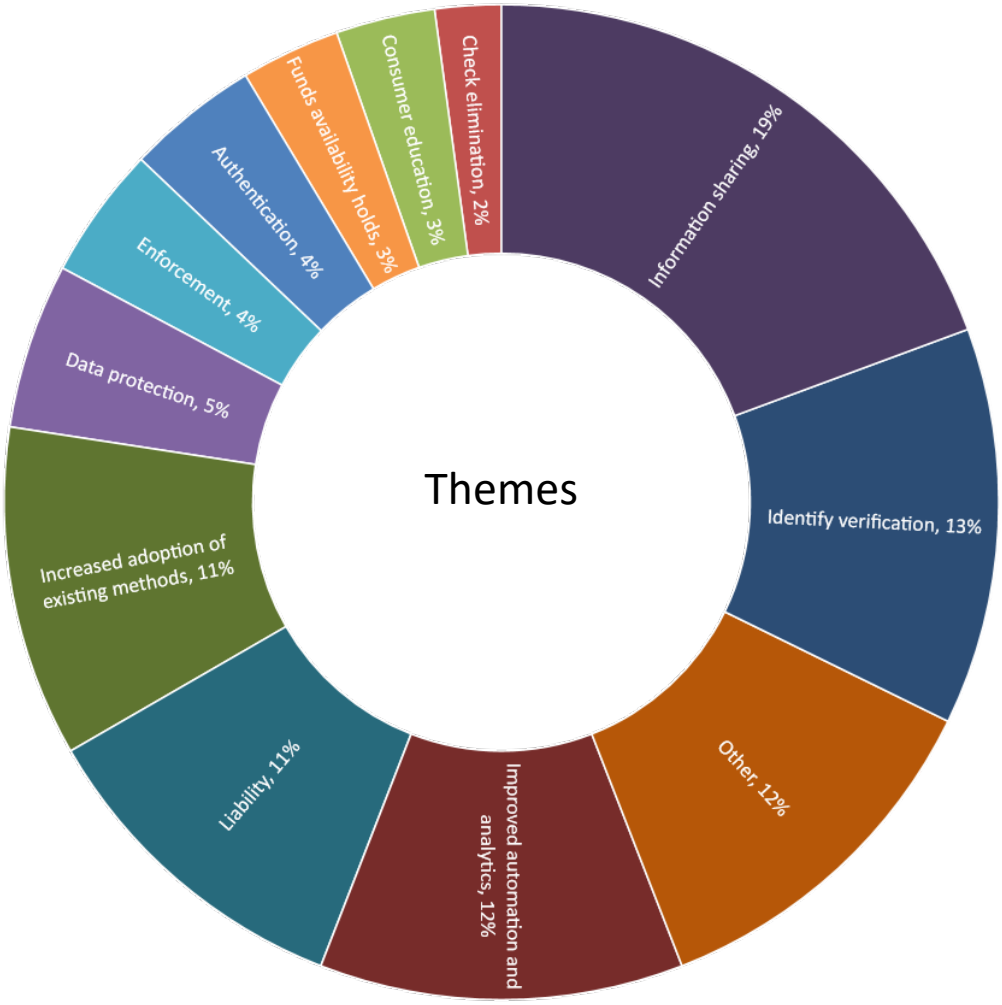
1. Information Sharing
   - Comprehensive database and alerting
   - Tracking system to determine source of fraud
   - Latest fraud schemes and how to mitigate
   - More sharing of information and cooperation among FIs
   - Ability to share information without breaking privacy rules
2. Identity Verification
   - Merchant participation in ID verification
   - KYC responsibility on those that accept payments
   - Online purchase identify verification
   - Name verification on ACH transactions to name on file on FI account



New or Improved Methods Needed Continued

Themes and examples continued:

3. Improved automation and analytics
   - Better automation and advanced tool; less reliance on multiple “home grown” tools and labor intense processes
   - Machine learning, predictive tools
   - Improved core system analytics
   - Real-time tools
4. Liability
   - Additional responsibility and accountability on merchant accepting card as payment
   - Greater accountability on business/merchant for data breaches
5. Increased adoption of existing methods
   - Stricter endorsement requirements/mandates on RDC items
   - Greater adoption of EMV readers by merchants and automated fuel dispensers
   - Reduce use of mag stripe fallback by merchants when chip card can’t be read at terminal
   - Require PIN on debit and credit card transactions



Data Tables

Note: Figures may not sum due to rounding.

Data Tables

What types of customers are the predominant users of your financial institution's payment products and services?

		Respondent Size - Total Assets in Millions of Dollars			
	Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Both somewhat even	25%	6%	26%	33%	57%
Primarily business/ commercial	5%	-	3%	11%	9%
Primarily consumers	70%	94%	71%	57%	35%

Which of the following payments products does your financial institution offer?

		Respondent Size - Total Assets in Millions of Dollars			
	Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Cash	95%	90%	98%	95%	96%
Checks	99%	96%	100%	100%	100%
Credit cards	43%	51%	38%	42%	42%
Debit cards	94%	83%	99%	99%	100%
Prepaid cards	42%	39%	43%	45%	38%
ACH origination	69%	39%	71%	89%	92%
ACH receipt	96%	93%	98%	96%	96%
Wire transfers	93%	79%	98%	100%	100%
International payments	32%	9%	28%	49%	71%
Bill payments	82%	51%	91%	98%	100%
Person to person (P2P) payments	45%	17%	44%	64%	79%
Consumer remote deposit capture	57%	21%	57%	80%	96%
Business remote deposit capture	44%	5%	41%	72%	92%

Did your financial institution experience any payment fraud attempts in 2016?

		Respondent Size - Total Assets in Millions of Dollars			
	Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Yes	82%	57%	88%	95%	100%
No	16%	38%	11%	4%	-
Don't know	2%	5%	1%	1%	-

Indicate the payment types where your financial institution experienced the highest number of fraud attempts in 2016. Consider all attempts regardless of actual financial losses. Select and rank the three that are highest.

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Checks	**1st Choice**	14%	7%	9%	18%	29%
	2nd Choice	21%	19%	19%	22%	33%
	3rd Choice	31%	26%	35%	36%	14%
Credit cards	**1st Choice**	4%	7%	1%	3%	14%
	2nd Choice	15%	33%	11%	11%	5%
	3rd Choice	11%	9%	12%	11%	10%
Debit cards - PIN based	**1st Choice**	11%	16%	8%	11%	10%
	2nd Choice	32%	19%	41%	30%	33%
	3rd Choice	19%	26%	11%	22%	24%
Debit cards - signature based	**1st Choice**	68%	67%	76%	66%	48%
	2nd Choice	18%	16%	15%	20%	24%
	3rd Choice	5%	-	3%	8%	10%
ACH credits	**1st Choice**	-	-	-	-	-
	2nd Choice	-	-	1%	-	-
	3rd Choice	2%	2%	4%	-	5%
ACH debits	**1st Choice**	1%	2%	1%	-	-
	2nd Choice	5%	5%	5%	5%	-
	3rd Choice	10%	9%	12%	4%	24%
Wires	**1st Choice**	1%	-	1%	3%	-
	2nd Choice	4%	2%	1%	8%	5%
	3rd Choice	7%	2%	5%	7%	19%

Did your financial institution experience any payment fraud losses in 2016?

		Respondent Size - Total Assets in Millions of Dollars			
	Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Yes	75%	46%	85%	83%	100%
No	22%	45%	13%	14%	-
Don't know	4%	9%	2%	2%	-

On which payment types did fraud losses occur?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Checks	**Losses**	74%	48%	61%	89%	100%
	No Losses	23%	48%	33%	11%	-
	Don't Know	3%	4%	6%	-	-
Credit cards	**Losses**	77%	84%	74%	70%	90%
	No Losses	16%	11%	19%	19%	10%
	Don't Know	7%	5%	7%	11%	-
Debit cards - PIN based	**Losses**	81%	78%	70%	91%	92%
	No Losses	14%	19%	24%	4%	8%
	Don't Know	5%	4%	6%	5%	-
Debit cards - signature based	**Losses**	96%	97%	96%	96%	96%
	No Losses	2%	-	3%	3%	-
	Don't Know	2%	3%	1%	1%	4%
ACH credits	**Losses**	8%	11%	2%	5%	25%
	No Losses	86%	89%	94%	87%	60%
	Don't Know	6%	-	4%	8%	15%
ACH debits	**Losses**	23%	23%	16%	15%	57%
	No Losses	69%	73%	80%	75%	29%
	Don't Know	8%	5%	4%	10%	14%
Wires	**Losses**	13%	-	10%	9%	36%
	No Losses	84%	100%	86%	91%	55%
	Don't Know	3%	-	4%	-	9%
Prepaid cards	**Losses**	7%	-	5%	5%	25%
	No Losses	86%	100%	86%	95%	50%
	Don't Know	7%	-	9%	-	25%

For your financial institution, how have losses due to payments fraud changed in 2016 compared to 2015?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Checks	**Increased**	28%	28%	13%	30%	61%
	Stayed the Same	47%	60%	57%	40%	26%
	Decreased	20%	12%	20%	25%	13%
	Don't Know	5%	-	10%	5%	-
Credit cards	**Increased**	41%	53%	29%	38%	60%
	Stayed the Same	32%	35%	29%	33%	30%
	Decreased	16%	12%	21%	17%	10%
	Don't Know	11%	-	21%	13%	-
Debit cards - PIN based	**Increased**	50%	68%	35%	55%	61%
	Stayed the Same	33%	32%	40%	28%	22%
	Decreased	12%	-	15%	11%	17%
	Don't Know	6%	-	10%	6%	-
Debit cards - signature based	**Increased**	63%	68%	58%	61%	77%
	Stayed the Same	19%	24%	18%	22%	5%
	Decreased	15%	9%	16%	15%	18%
	Don't Know	4%	-	8%	1%	-
ACH credits	**Increased**	2%	6%	-	-	6%
	Stayed the Same	83%	88%	82%	85%	75%
	Decreased	4%	-	2%	3%	13%
	Don't Know	12%	6%	16%	12%	6%
ACH debits	**Increased**	8%	15%	6%	-	24%
	Stayed the Same	79%	80%	81%	88%	53%
	Decreased	4%	-	2%	3%	18%
	Don't Know	8%	5%	10%	9%	6%
Wires	**Increased**	10%	-	5%	8%	30%
	Stayed the Same	77%	93%	77%	78%	65%
	Decreased	3%	7%	2%	3%	5%
	Don't Know	10%	-	16%	11%	-
Prepaid cards	**Increased**	6%	-	-	5%	40%
	Stayed the Same	76%	100%	68%	79%	60%
	Decreased	-	-	-	-	-
	Don't Know	18%	-	32%	16%	-

At your financial institution is fraud prevention/investigation a centralized function, is it decentralized by payment channel/silo, or is it some of each?

		Respondent Size - Total Assets in Millions of Dollars			
	Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Centralized	58%	69%	57%	54%	33%
Decentralized	12%	7%	15%	13%	17%
Mixed	30%	23%	28%	33%	50%

If mixed, which payment channels are managed separately?

		Respondent Size - Total Assets in Millions of Dollars			
	Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
ACH	15%	19%	12%	9%	21%
Checks	19%	21%	23%	13%	21%
Credit card	16%	17%	12%	20%	10%
Debit card	34%	29%	40%	35%	28%
Prepaid card	4%	3%	4%	6%	3%
Wires	13%	10%	9%	17%	17%

Which of the following account application processes does your financial institution use to mitigate risks when establishing new demand deposit or transaction accounts?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Conduct KYC and CIP review	**Use and Very Effective**	65%	55%	67%	70%	75%
	Use and Somewhat effective	23%	23%	21%	26%	25%
	Use and somewhat ineffective	3%	3%	7%	1%	-
	Don't Use	5%	13%	4%	1%	-
	Don't Know	3%	7%	1%	1%	-
Establish exposure limits for customer use of payment products	**Use and Very Effective**	45%	30%	39%	62%	52%
	Use and Somewhat effective	37%	29%	47%	34%	35%
	Use and somewhat ineffective	4%	6%	4%	-	9%
	Don't Use	11%	23%	9%	3%	4%
	Don't Know	4%	12%	1%	1%	-
Identity verification services to help confirm the identity of the person or business	**Use and Very Effective**	50%	45%	51%	50%	58%
	Use and Somewhat effective	26%	16%	25%	32%	38%
	Use and somewhat ineffective	1%	1%	1%	1%	-
	Don't Use	21%	32%	21%	17%	4%
	Don't Know	2%	6%	1%	-	-
Agreements that specify minimum security requirements for online banking pymt. origination	**Use and Very Effective**	39%	32%	41%	42%	38%
	Use and Somewhat effective	30%	18%	33%	38%	25%
	Use and somewhat ineffective	8%	5%	9%	7%	17%
	Don't Use	16%	32%	11%	10%	13%
	Don't Know	7%	14%	6%	3%	8%
New customer limited to in person submission of new account application	**Use and Very Effective**	58%	61%	65%	57%	25%
	Use and Somewhat effective	16%	14%	12%	21%	21%
	Use and somewhat ineffective	-	-	-	-	-
	Don't Use	24%	23%	19%	20%	54%
	Don't Know	3%	3%	4%	3%	-
Credit report inquiry	**Use and Very Effective**	33%	38%	28%	39%	13%
	Use and Somewhat effective	27%	26%	30%	21%	35%
	Use and somewhat ineffective	2%	3%	1%	3%	-
	Don't Use	38%	32%	40%	38%	48%
	Don't Know	1%	1%	1%	-	4%
Establish prefunding requirements for customer use of payment products	**Use and Very Effective**	23%	14%	23%	31%	29%
	Use and Somewhat effective	13%	9%	16%	14%	8%
	Use and somewhat ineffective	3%	2%	1%	3%	8%
	Don't Use	51%	63%	48%	47%	46%
	Don't Know	10%	13%	13%	6%	8%
Financial or tax return review	**Use and Very Effective**	15%	13%	15%	17%	13%
	Use and Somewhat effective	14%	13%	17%	14%	9%
	Use and somewhat ineffective	3%	4%	1%	3%	4%
	Don't Use	64%	63%	66%	62%	65%
	Don't Know	4%	6%	1%	4%	9%
Use of positive and negative lists, e.g., NACHA originator watch list	**Use and Very Effective**	12%	12%	10%	14%	17%
	Use and Somewhat effective	13%	13%	13%	10%	22%
	Use and somewhat ineffective	4%	3%	3%	8%	-
	Don't Use	61%	54%	69%	60%	61%
	Don't Know	9%	18%	5%	8%	-
Require a reserve of funds for return items and other claims	**Use and Very Effective**	5%	6%	8%	-	4%
	Use and Somewhat effective	9%	9%	10%	7%	8%
	Use and somewhat ineffective	1%	-	1%	1%	-
	Don't Use	76%	69%	74%	84%	75%
	Don't Know	10%	15%	8%	8%	13%

Which of the following account application processes does your financial institution use to mitigate credit card fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Credit report inquiry during credit card account application process	**Use and Very Effective**	68%	78%	52%	76%	44%
	Use and Somewhat effective	23%	15%	34%	21%	33%
	Use and somewhat ineffective	4%	5%	7%	-	11%
	Don't Use	2%	2%	3%	-	-
	Don't Know	3%	-	3%	3%	11%
Credit underwriting review	**Use and Very Effective**	58%	49%	50%	78%	56%
	Use and Somewhat effective	23%	28%	29%	13%	22%
	Use and somewhat ineffective	6%	8%	11%	3%	-
	Don't Use	6%	10%	4%	3%	11%
	Don't Know	6%	5%	7%	3%	11%
Identity verification services to help confirm the identity of the person or business during the account application process	**Use and Very Effective**	60%	63%	55%	68%	33%
	Use and Somewhat effective	17%	8%	24%	15%	44%
	Use and somewhat ineffective	4%	3%	3%	6%	-
	Don't Use	17%	25%	14%	12%	11%
	Don't Know	3%	3%	3%	-	11%
Financial or tax return review	**Use and Very Effective**	30%	36%	25%	31%	11%
	Use and Somewhat effective	21%	21%	18%	25%	22%
	Use and somewhat ineffective	5%	8%	4%	3%	-
	Don't Use	34%	33%	46%	22%	44%
	Don't Know	10%	3%	7%	19%	22%
Collateral pledge against activity on credit card account	**Use and Very Effective**	17%	22%	7%	23%	-
	Use and Somewhat effective	14%	11%	11%	20%	11%
	Use and somewhat ineffective	6%	5%	4%	3%	22%
	Don't Use	56%	57%	70%	43%	56%
	Don't Know	8%	5%	7%	10%	11%

What are the three current fraud attacks most often used to initiate debit card fraud against your financial institution or your customer's accounts?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Counterfeit debit cards used at point-of-sale	**1st Choice**	57%	51%	53%	64%	70%
	2nd Choice	20%	15%	24%	19%	22%
	3rd Choice	7%	9%	8%	6%	-
Counterfeit or stolen cards or card data used online (card-not-present)	**1st Choice**	34%	40%	40%	25%	26%
	2nd Choice	34%	18%	30%	47%	39%
	3rd Choice	14%	16%	14%	14%	13%
Debit card used by family member or friend	**1st Choice**	3%	4%	3%	3%	-
	2nd Choice	4%	4%	6%	4%	-
	3rd Choice	25%	25%	26%	26%	17%
Lost or stolen debit cards used at point-of-sale	**1st Choice**	4%	2%	5%	5%	4%
	2nd Choice	11%	20%	10%	8%	9%
	3rd Choice	14%	15%	14%	14%	13%
Counterfeit or stolen cards or card data used in telephone or mail order (card-not-present)	**1st Choice**	2%	2%	4%	-	-
	2nd Choice	14%	27%	14%	8%	9%
	3rd Choice	13%	11%	19%	9%	9%
Counterfeit debit cards used at ATM, e.g., for cash withdrawal	**1st Choice**	1%	2%	1%	1%	-
	2nd Choice	13%	16%	13%	9%	17%
	3rd Choice	14%	7%	10%	19%	26%
Account takeover of customers' accounts, e.g., changes cardholders address/contact data, takeover of merchant account with card-on-file, etc.	**1st Choice**	-	-	-	1%	-
	2nd Choice	1%	-	1%	1%	-
	3rd Choice	3%	2%	-	4%	17%
Identity theft or synthetic identity theft used to establish new debit card account/demand deposit accounts or defraud existing accounts	**1st Choice**	-	-	-	-	-
	2nd Choice	3%	-	1%	1%	-
	3rd Choice	1%	5%	1%	4%	-
Lost or stolen debit cards used at ATM	**1st Choice**	-	-	1%	-	-
	2nd Choice	1%	-	-	1%	4%
	3rd Choice	3%	4%	3%	1%	4%
Fraudulent credentials or other data used to establish new debit card accounts or to defraud existing accounts	**1st Choice**	-	-	-	-	-
	2nd Choice	1%	-	1%	1%	-
	3rd Choice	1%	2%	1%	-	-

Which of the following transaction authentication methods does your financial institution use to mitigate debit card fraud risks?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
PIN authentication	**Use and Very Effective**	53%	54%	51%	55%	54%
	Use and Somewhat effective	38%	37%	40%	39%	33%
	Use and somewhat ineffective	5%	4%	6%	4%	8%
	Don't Use	1%	-	1%	1%	-
	Don't Know	3%	6%	2%	0%	4%
Magnetic stripe authentication	**Use and Very Effective**	22%	32%	21%	21%	9%
	Use and Somewhat effective	50%	51%	50%	53%	35%
	Use and somewhat ineffective	20%	9%	19%	21%	48%
	Don't Use	4%	-	6%	4%	4%
	Don't Know	4%	8%	4%	1%	4%
Card security code verified during transaction authorization	**Use and Very Effective**	39%	56%	30%	42%	22%
	Use and Somewhat effective	47%	37%	52%	46%	57%
	Use and somewhat ineffective	4%	2%	4%	4%	13%
	Don't Use	5%	2%	8%	5%	4%
	Don't Know	4%	4%	6%	3%	4%
Card chip authentication	**Use and Very Effective**	43%	30%	46%	48%	43%
	Use and Somewhat effective	37%	41%	32%	39%	39%
	Use and somewhat ineffective	2%	-	2%	1%	4%
	Don't Use	16%	26%	16%	10%	9%
	Don't Know	3%	4%	4%	1%	4%
Card holder address verified during transaction authorization	**Use and Very Effective**	23%	39%	15%	21%	17%
	Use and Somewhat effective	36%	31%	33%	43%	35%
	Use and somewhat ineffective	11%	8%	14%	9%	13%
	Don't Use	21%	12%	24%	20%	30%
	Don't Know	9%	10%	13%	7%	4%
Out-of-band authentication for transactions identifed as high risk	**Use and Very Effective**	18%	12%	20%	24%	13%
	Use and Somewhat effective	22%	25%	23%	18%	29%
	Use and somewhat ineffective	3%	6%	4%	1%	-
	Don't Use	32%	27%	29%	33%	46%
	Don't Know	24%	31%	24%	24%	13%
3D Secure or its equivalent for online payments	**Use and Very Effective**	3%	4%	3%	3%	-
	Use and Somewhat effective	11%	10%	7%	19%	9%
	Use and somewhat ineffective	4%	-	-	6%	22%
	Don't Use	56%	50%	64%	54%	48%
	Don't Know	26%	37%	26%	19%	22%

Which of the following data does your financial institution incorporate into fraud screening tools to mitigate debit card fraud risk?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Out of pattern activity	**Use and Very Effective**	43%	50%	39%	45%	38%
	Use and Somewhat effective	44%	33%	48%	48%	50%
	Use and somewhat ineffective	7%	13%	6%	3%	4%
	Don't Use	2%	-	3%	4%	-
	Don't Know	4%	4%	5%	-	8%
Block/score transactions from countries perceived as high risk	**Use and Very Effective**	64%	62%	60%	74%	54%
	Use and Somewhat effective	26%	19%	31%	22%	38%
	Use and somewhat ineffective	1%	4%	-	1%	-
	Don't Use	4%	8%	5%	1%	4%
	Don't Know	4%	8%	4%	1%	4%
Transaction value	**Use and Very Effective**	27%	30%	27%	27%	17%
	Use and Somewhat effective	45%	36%	44%	48%	63%
	Use and somewhat ineffective	9%	9%	10%	7%	13%
	Don't Use	9%	8%	9%	14%	-
	Don't Know	9%	17%	9%	4%	8%
Common point of compromise	**Use and Very Effective**	25%	30%	18%	28%	25%
	Use and Somewhat effective	42%	30%	39%	52%	50%
	Use and somewhat ineffective	11%	14%	14%	3%	17%
	Don't Use	9%	10%	15%	6%	-
	Don't Know	13%	16%	15%	11%	8%
Merchant category code, card acceptor ID, etc.	**Use and Very Effective**	24%	22%	22%	31%	13%
	Use and Somewhat effective	45%	36%	42%	51%	61%
	Use and somewhat ineffective	8%	14%	10%	1%	9%
	Don't Use	10%	12%	13%	4%	13%
	Don't Know	13%	16%	13%	13%	4%
Behavior analytics	**Use and Very Effective**	30%	28%	29%	30%	33%
	Use and Somewhat effective	40%	26%	36%	49%	54%
	Use and somewhat ineffective	5%	8%	6%	1%	4%
	Don't Use	12%	18%	13%	10%	-
	Don't Know	14%	20%	17%	9%	8%
Velocity of transactions	**Use and Very Effective**	24%	25%	22%	31%	4%
	Use and Somewhat effective	42%	29%	36%	46%	75%
	Use and somewhat ineffective	8%	10%	9%	4%	8%
	Don't Use	14%	16%	19%	10%	8%
	Don't Know	12%	20%	14%	9%	4%
Positive and negative lists	**Use and Very Effective**	12%	21%	9%	9%	13%
	Use and Somewhat effective	19%	15%	20%	19%	25%
	Use and somewhat ineffective	5%	6%	5%	6%	-
	Don't Use	33%	27%	31%	34%	46%
	Don't Know	31%	31%	34%	31%	17%
Device velocity checks	**Use and Very Effective**	12%	14%	10%	13%	13%
	Use and Somewhat effective	21%	20%	15%	25%	25%
	Use and somewhat ineffective	2%	6%	-	-	4%
	Don't Use	33%	18%	38%	40%	25%
	Don't Know	33%	41%	37%	22%	33%

Which of the following reporting and other risk management methods does your financial institution use to mitigate debit card fraud risk?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Provide customers online information services to view transactions, statements, etc.	**Use and Very Effective**	52%	58%	51%	55%	38%
	Use and Somewhat effective	43%	35%	48%	38%	58%
	Use and somewhat ineffective	2%	-	-	5%	-
	Don't Use	3%	8%	1%	-	-
	Don't Know	-	-	-	1%	4%
Provide staff education and training on debit card fraud risk mitigation	**Use and Very Effective**	24%	29%	24%	21%	17%
	Use and Somewhat effective	59%	54%	58%	66%	58%
	Use and somewhat ineffective	13%	10%	15%	13%	17%
	Don't Use	2%	6%	1%	-	4%
	Don't Know	1%	2%	1%	-	4%
Block and reissue all cards known to be on breached card list	**Use and Very Effective**	59%	72%	61%	51%	46%
	Use and Somewhat effective	26%	13%	25%	30%	42%
	Use and somewhat ineffective	3%	6%	3%	4%	-
	Don't Use	11%	8%	10%	15%	8%
	Don't Know	1%	2%	1%	-	4%
Provide customer education and training on fraud risk mitigation	**Use and Very Effective**	11%	16%	12%	9%	8%
	Use and Somewhat effective	41%	39%	40%	45%	38%
	Use and somewhat ineffective	30%	27%	34%	30%	25%
	Don't Use	13%	18%	9%	12%	17%
	Don't Know	5%	-	5%	4%	13%
Manual review of suspicious transactions	**Use and Very Effective**	31%	33%	31%	32%	21%
	Use and Somewhat effective	36%	37%	40%	32%	38%
	Use and somewhat ineffective	14%	12%	12%	18%	13%
	Don't Use	15%	16%	13%	17%	17%
	Don't Know	4%	2%	4%	1%	13%
Provide customers alerts via text, email, or within application	**Use and Very Effective**	35%	31%	34%	39%	33%
	Use and Somewhat effective	30%	14%	34%	36%	33%
	Use and somewhat ineffective	9%	10%	9%	10%	4%
	Don't Use	23%	37%	22%	15%	25%
	Don't Know	3%	8%	1%	-	4%
Apply heightened monitoring and selectively block and reissue cards known to be on breached card list	**Use and Very Effective**	34%	43%	30%	32%	29%
	Use and Somewhat effective	31%	22%	32%	38%	29%
	Use and somewhat ineffective	5%	4%	5%	7%	-
	Don't Use	27%	27%	29%	23%	33%
	Don't Know	3%	4%	4%	-	8%
Limit load value on prepaid cards	**Use and Very Effective**	32%	42%	26%	37%	11%
	Use and Somewhat effective	30%	25%	23%	33%	56%
	Use and somewhat ineffective	7%	4%	10%	4%	11%
	Don't Use	22%	17%	29%	22%	11%
	Don't Know	10%	13%	13%	4%	11%
Outsource debit card fraud management (no internal tools or expertise)	**Use and Very Effective**	37%	43%	32%	38%	26%
	Use and Somewhat effective	24%	20%	31%	24%	14%
	Use and somewhat ineffective	4%	6%	4%	1%	5%
	Don't Use	29%	20%	30%	32%	41%
	Don't Know	6%	12%	3%	4%	5%
Allow customer to turn card off when not in use	**Use and Very Effective**	16%	10%	18%	21%	8%
	Use and Somewhat effective	15%	6%	16%	20%	21%
	Use and somewhat ineffective	6%	2%	4%	7%	17%
	Don't Use	60%	75%	61%	52%	46%
	Don't Know	3%	8%	1%	-	8%

Continued - Which of the following reporting and other risk management methods does your financial institution use to mitigate debit card fraud risk?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Only issue non-reloadable prepaid cards	**Use and Very Effective**	18%	17%	16%	27%	0%
	Use and Somewhat effective	11%	9%	13%	12%	11%
	Use and somewhat ineffective	2%	4%	-	4%	-
	Don't Use	60%	65%	59%	54%	67%
	Don't Know	9%	4%	13%	4%	22%
Provide customers online services to dispute transactions	**Use and Very Effective**	7%	10%	4%	8%	8%
	Use and Somewhat effective	11%	12%	8%	11%	17%
	Use and somewhat ineffective	5%	2%	4%	7%	4%
	Don't Use	75%	71%	83%	74%	67%
	Don't Know	2%	6%	1%	-	4%

What are the three current fraud attacks most often used to initiate credit card fraud against your financial institution or your customer's accounts?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Counterfeit or stolen cards or card data used online (card-not-present)	**1st Choice**	38%	34%	38%	40%	44%
	2nd Choice	39%	40%	46%	33%	33%
	3rd Choice	12%	14%	4%	17%	11%
Counterfeit credit cards used at point-of-sale	**1st Choice**	53%	42%	62%	57%	56%
	2nd Choice	20%	14%	19%	23%	33%
	3rd Choice	6%	6%	12%	3%	-
Counterfeit or stolen cards or card data used by telephone or mail order (card-not-present)	**1st Choice**	3%	9%	-	-	-
	2nd Choice	12%	17%	12%	10%	-
	3rd Choice	20%	23%	31%	13%	-
Lost or stolen credit cards used at point-of-sale	**1st Choice**	2%	3%	-	3%	-
	2nd Choice	13%	14%	15%	13%	-
	3rd Choice	19%	20%	15%	27%	-
Credit card used by family member or friend	**1st Choice**	-	-	-	-	-
	2nd Choice	4%	3%	4%	3%	11%
	3rd Choice	19%	23%	23%	10%	22%
Counterfeit credit cards used at ATM, e.g., for cash advance	**1st Choice**	2%	6%	-	-	-
	2nd Choice	6%	9%	4%	7%	-
	3rd Choice	5%	9%	-	3%	11%
Account takeover of customers' accounts, e.g., changes cardholders address/contact data, takeover of merchant account with card-on-file, etc.	**1st Choice**	-	-	-	-	-
	2nd Choice	1%	-	-	3%	-
	3rd Choice	5%	-	4%	3%	33%
Fraudulent credentials or other data used to establish new credit card accounts or to defraud existing accounts	**1st Choice**	-	-	-	-	-
	2nd Choice	3%	3%	-	-	22%
	3rd Choice	1%	1%	-	-	11%
Lost or stolen credit cards used at ATM	**1st Choice**	-	3%	-	-	-
	2nd Choice	1%	-	-	-	-
	3rd Choice	2%	-	4%	3%	-
Identity theft or synthetic identity theft used to establish new credit card accounts or to defraud existing accounts	**1st Choice**	-	-	-	-	-
	2nd Choice	-	-	-	-	-
	3rd Choice	3%	-	4%	7%	-

Which of the following transaction authentication methods does your financial institution use to mitigate credit card fraud risks?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Card security code verified during transaction authorization	**Use and Very Effective**	46%	53%	42%	41%	44%
	Use and Somewhat effective	40%	36%	35%	53%	22%
	Use and somewhat ineffective	9%	8%	15%	-	22%
	Don't Use	2%	-	8%	-	-
	Don't Know	4%	3%	-	6%	11%
Card chip authentication	**Use and Very Effective**	47%	45%	54%	50%	22%
	Use and Somewhat effective	38%	34%	42%	41%	33%
	Use and somewhat ineffective	7%	11%	4%	-	22%
	Don't Use	6%	8%	-	6%	11%
	Don't Know	3%	3%	-	3%	11%
Magnetic stripe authentication	**Use and Very Effective**	20%	30%	15%	16%	11%
	Use and Somewhat effective	45%	41%	46%	53%	33%
	Use and somewhat ineffective	24%	22%	31%	16%	44%
	Don't Use	2%	-	-	6%	-
	Don't Know	9%	8%	8%	9%	11%
PIN authentication	**Use and Very Effective**	41%	50%	38%	42%	11%
	Use and Somewhat effective	38%	42%	42%	30%	33%
	Use and somewhat ineffective	6%	6%	4%	3%	22%
	Don't Use	8%	3%	8%	12%	11%
	Don't Know	8%	-	8%	12%	22%
Card holder address verified during transaction authorization	**Use and Very Effective**	32%	39%	31%	21%	44%
	Use and Somewhat effective	40%	39%	42%	48%	11%
	Use and somewhat ineffective	10%	8%	8%	12%	11%
	Don't Use	11%	8%	12%	9%	22%
	Don't Know	8%	6%	8%	9%	11%
Out-of-band authentication for transactions identified as high risk	**Use and Very Effective**	15%	12%	8%	28%	11%
	Use and Somewhat effective	22%	18%	16%	28%	33%
	Use and somewhat ineffective	7%	12%	8%	3%	-
	Don't Use	23%	21%	32%	17%	22%
	Don't Know	33%	38%	36%	24%	33%
3D Secure or its equivalent for online payments	**Use and Very Effective**	4%	6%	-	4%	11%
	Use and Somewhat effective	7%	9%	8%	7%	-
	Use and somewhat ineffective	8%	11%	4%	4%	22%
	Don't Use	43%	37%	50%	41%	56%
	Don't Know	37%	37%	38%	44%	11%

Which of the following data does your financial institution incorporate into fraud screening tools to mitigate credit card fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Out of pattern activity	**Use and Very Effective**	45%	50%	38%	48%	33%
	Use and Somewhat effective	42%	36%	50%	39%	56%
	Use and somewhat ineffective	3%	-	4%	6%	-
	Don't Use	1%	-	4%	-	-
	Don't Know	9%	14%	4%	6%	11%
Block/score transactions from countries perceived as high risk	**Use and Very Effective**	67%	56%	65%	82%	67%
	Use and Somewhat effective	19%	22%	27%	9%	22%
	Use and somewhat ineffective	3%	6%	-	3%	-
	Don't Use	4%	8%	4%	-	-
	Don't Know	7%	8%	4%	6%	11%
Transaction value	**Use and Very Effective**	20%	23%	12%	26%	11%
	Use and Somewhat effective	48%	34%	58%	52%	67%
	Use and somewhat ineffective	10%	11%	12%	7%	11%
	Don't Use	3%	6%	4%	-	-
	Don't Know	19%	26%	15%	15%	11%
Behavior analytics	**Use and Very Effective**	35%	34%	35%	34%	44%
	Use and Somewhat effective	38%	29%	46%	41%	44%
	Use and somewhat ineffective	3%	3%	4%	3%	-
	Don't Use	7%	14%	4%	3%	-
	Don't Know	16%	20%	12%	17%	11%
Merchant category code, card acceptor ID, etc.	**Use and Very Effective**	25%	23%	19%	38%	11%
	Use and Somewhat effective	38%	29%	38%	41%	67%
	Use and somewhat ineffective	10%	9%	15%	7%	11%
	Don't Use	6%	9%	12%	-	-
	Don't Know	20%	31%	15%	14%	11%
Common point of compromise	**Use and Very Effective**	26%	27%	15%	34%	22%
	Use and Somewhat effective	33%	24%	35%	34%	56%
	Use and somewhat ineffective	13%	12%	19%	10%	11%
	Don't Use	7%	12%	12%	-	-
	Don't Know	21%	24%	19%	21%	11%
Velocity of transactions	**Use and Very Effective**	27%	26%	23%	28%	33%
	Use and Somewhat effective	39%	29%	38%	48%	44%
	Use and somewhat ineffective	6%	9%	-	10%	-
	Don't Use	7%	9%	12%	3%	-
	Don't Know	21%	26%	27%	10%	22%
Positive and negative lists	**Use and Very Effective**	18%	18%	16%	17%	22%
	Use and Somewhat effective	17%	15%	24%	14%	11%
	Use and somewhat ineffective	4%	6%	4%	3%	-
	Don't Use	29%	30%	20%	31%	44%
	Don't Know	32%	30%	36%	34%	22%
Device velocity checks	**Use and Very Effective**	10%	6%	8%	12%	22%
	Use and Somewhat effective	18%	21%	20%	15%	11%
	Use and somewhat ineffective	4%	3%	8%	4%	-
	Don't Use	29%	27%	24%	35%	33%
	Don't Know	38%	42%	40%	35%	33%

Which of the following reporting and other risk management methods does your financial institution use to mitigate credit card fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Provide customers online information services to view transactions, statements, etc.	**Use and Very Effective**	49%	53%	40%	53%	44%
	Use and Somewhat effective	43%	38%	52%	44%	33%
	Use and somewhat ineffective	4%	6%	-	3%	11%
	Don't Use	3%	3%	8%	-	-
	Don't Know	1%	-	-	-	11%
Provide staff education and training on credit card fraud risk mitigation	**Use and Very Effective**	29%	27%	24%	38%	22%
	Use and Somewhat effective	42%	48%	48%	34%	33%
	Use and somewhat ineffective	15%	9%	20%	19%	11%
	Don't Use	9%	15%	-	6%	22%
	Don't Know	4%	-	8%	3%	11%
Block and reissue all cards known to be on breached card list	**Use and Very Effective**	57%	64%	56%	55%	44%
	Use and Somewhat effective	22%	18%	28%	21%	22%
	Use and somewhat ineffective	6%	6%	8%	6%	-
	Don't Use	11%	6%	8%	18%	11%
	Don't Know	4%	6%	-	-	22%
Manual review of suspicious transactions	**Use and Very Effective**	33%	36%	32%	32%	22%
	Use and Somewhat effective	36%	33%	44%	32%	33%
	Use and somewhat ineffective	9%	3%	8%	10%	33%
	Don't Use	15%	24%	8%	16%	-
	Don't Know	7%	3%	8%	10%	11%
Provide customers alerts via text, email, or within application	**Use and Very Effective**	41%	44%	28%	48%	44%
	Use and Somewhat effective	28%	13%	44%	29%	33%
	Use and somewhat ineffective	6%	3%	8%	6%	11%
	Don't Use	20%	41%	12%	10%	-
	Don't Know	5%	-	8%	6%	11%
Provide customer education and training on risk mitigation	**Use and Very Effective**	11%	16%	8%	11%	-
	Use and Somewhat effective	29%	28%	32%	29%	22%
	Use and somewhat ineffective	31%	31%	40%	18%	44%
	Don't Use	22%	25%	8%	32%	22%
	Don't Know	7%	-	12%	11%	11%
Outsource card fraud management (no internal tools or expertise)	**Use and Very Effective**	44%	42%	40%	48%	44%
	Use and Somewhat effective	22%	18%	36%	10%	33%
	Use and somewhat ineffective	3%	3%	-	7%	-
	Don't Use	21%	24%	16%	24%	11%
	Don't Know	10%	12%	8%	10%	11%
Apply heightened monitoring and selectively block and reissue cards known to be on breached card list	**Use and Very Effective**	27%	33%	21%	31%	11%
	Use and Somewhat effective	36%	30%	54%	17%	67%
	Use and somewhat ineffective	4%	-	-	14%	-
	Don't Use	22%	27%	21%	21%	11%
	Don't Know	11%	9%	4%	17%	11%
Provide customers online services to dispute transactions	**Use and Very Effective**	17%	26%	-	23%	11%
	Use and Somewhat effective	18%	15%	8%	30%	22%
	Use and somewhat ineffective	10%	12%	16%	7%	-
	Don't Use	49%	47%	72%	33%	44%
	Don't Know	5%	-	4%	7%	22%
Allow customer to turn card off when not in use	**Use and Very Effective**	13%	6%	12%	23%	11%
	Use and Somewhat effective	5%	6%	4%	3%	11%
	Use and somewhat ineffective	3%	3%	4%	-	11%
	Don't Use	71%	79%	72%	67%	56%
	Don't Know	7%	6%	8%	7%	11%

What are the three current fraud attacks most often used to initiate check fraud against your financial institution or your customer's accounts?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Altered or forged checks presented for payment	**1st Choice**	22%	12%	23%	21%	17%
	2nd Choice	21%	17%	18%	25%	25%
	3rd Choice	13%	13%	11%	16%	17%
Counterfeit checks presented for payment	**1st Choice**	30%	23%	28%	37%	29%
	2nd Choice	13%	17%	11%	12%	17%
	3rd Choice	9%	8%	8%	11%	8%
Counterfeit checks deposited (over-the-counter, ATM, RDC, etc.)	**1st Choice**	20%	21%	16%	17%	38%
	2nd Choice	17%	17%	14%	23%	8%
	3rd Choice	9%	13%	3%	9%	13%
Check kiting	**1st Choice**	9%	15%	12%	5%	0%
	2nd Choice	8%	13%	7%	5%	8%
	3rd Choice	22%	29%	25%	23%	-
Altered or forged checks deposited (over-the-counter, ATM, RDC, etc.)	**1st Choice**	10%	4%	7%	16%	17%
	2nd Choice	17%	15%	16%	16%	33%
	3rd Choice	9%	8%	8%	9%	8%
Duplicate checks presented for payment	**1st Choice**	1%	2%	3%	-	-
	2nd Choice	6%	2%	9%	7%	-
	3rd Choice	6%	4%	11%	4%	4%
Duplicate checks deposited (over-the-counter, ATM, RDC, etc.)	**1st Choice**	3%	-	7%	1%	-
	2nd Choice	4%	6%	5%	3%	-
	3rd Choice	5%	2%	3%	9%	4%
Identity theft or synthetic identity theft used to establish new banking/demand deposit account or to defraud existing accounts	**1st Choice**	2%	2%	4%	-	-
	2nd Choice	1%	-	1%	1%	-
	3rd Choice	4%	4%	3%	1%	17%
Abuse of power of attorney to defraud vulnerable adult	**1st Choice**	-	-	-	-	-
	2nd Choice	3%	2%	4%	3%	-
	3rd Choice	4%	2%	3%	5%	4%
Account takeover of customers' accounts	**1st Choice**	-	-	-	-	-
	2nd Choice	2%	-	4%	-	4%
	3rd Choice	4%	-	1%	4%	21%
Business email compromise	**1st Choice**	1%	-	1%	1%	-
	2nd Choice	1%	-	1%	3%	-
	3rd Choice	3%	-	4%	3%	4%
Use of fraudulent credentials or other data to establish new accounts or to defraud existing accounts	**1st Choice**	-	-	-	-	-
	2nd Choice	1%	-	1%	-	4%
	3rd Choice	2%	2%	4%	1%	-

Which of the following transaction authentication methods does your financial institution use to mitigate check fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Access credentials for remote deposit capture	**Use and Very Effective**	43%	42%	42%	48%	29%
	Use and Somewhat effective	40%	33%	42%	40%	38%
	Use and somewhat ineffective	3%	8%	-	1%	13%
	Don't Use	9%	8%	13%	3%	17%
	Don't Know	5%	8%	2%	7%	4%
Signature verification	**Use and Very Effective**	34%	47%	29%	30%	29%
	Use and Somewhat effective	35%	30%	42%	33%	38%
	Use and somewhat ineffective	12%	10%	10%	11%	25%
	Don't Use	17%	10%	16%	26%	8%
	Don't Know	2%	3%	4%	-	-
Positive pay services	**Use and Very Effective**	14%	9%	5%	19%	33%
	Use and Somewhat effective	17%	13%	8%	20%	42%
	Use and somewhat ineffective	1%	-	-	3%	4%
	Don't Use	60%	60%	80%	52%	17%
	Don't Know	9%	17%	7%	6%	4%
Payee positive services	**Use and Very Effective**	3%	2%	1%	3%	8%
	Use and Somewhat effective	7%	10%	4%	9%	8%
	Use and somewhat ineffective	1%	-	1%	3%	-
	Don't Use	78%	69%	85%	76%	79%
	Don't Know	11%	19%	8%	9%	4%
Post no check services	**Use and Very Effective**	2%	-	3%	1%	4%
	Use and Somewhat effective	8%	4%	7%	6%	29%
	Use and somewhat ineffective	-	-	-	1%	-
	Don't Use	72%	75%	80%	72%	46%
	Don't Know	17%	12%	10%	19%	21%

Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate check fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Large dollar item review on deposited or paid items	**Use and Very Effective**	43%	43%	48%	42%	30%
	Use and Somewhat effective	37%	24%	39%	42%	48%
	Use and somewhat ineffective	9%	9%	6%	10%	17%
	Don't Use	8%	20%	3%	4%	4%
	Don't Know	3%	4%	4%	1%	-
Manual review	**Use and Very Effective**	30%	35%	33%	24%	29%
	Use and Somewhat effective	36%	29%	41%	42%	25%
	Use and somewhat ineffective	14%	9%	14%	18%	13%
	Don't Use	14%	16%	8%	13%	29%
	Don't Know	5%	11%	4%	3%	4%
Duplicate check detection on deposit items	**Use and Very Effective**	30%	18%	32%	39%	25%
	Use and Somewhat effective	33%	16%	35%	41%	38%
	Use and somewhat ineffective	7%	8%	5%	7%	13%
	Don't Use	25%	46%	24%	13%	21%
	Don't Know	4%	12%	4%	-	4%
Duplicate check detection on paid items	**Use and Very Effective**	30%	16%	32%	37%	38%
	Use and Somewhat effective	33%	20%	33%	41%	33%
	Use and somewhat ineffective	6%	8%	4%	7%	8%
	Don't Use	25%	41%	27%	13%	17%
	Don't Know	6%	16%	4%	1%	4%
Value of items deposited or paid	**Use and Very Effective**	19%	19%	23%	16%	17%
	Use and Somewhat effective	37%	27%	31%	48%	50%
	Use and somewhat ineffective	9%	10%	8%	11%	8%
	Don't Use	28%	37%	31%	21%	21%
	Don't Know	6%	8%	7%	3%	4%
Out of pattern activities	**Use and Very Effective**	19%	24%	22%	15%	13%
	Use and Somewhat effective	32%	29%	27%	31%	54%
	Use and somewhat ineffective	9%	5%	7%	15%	8%
	Don't Use	37%	35%	41%	38%	25%
	Don't Know	4%	7%	4%	1%	0%
Kite detection software	**Use and Very Effective**	19%	6%	22%	25%	22%
	Use and Somewhat effective	30%	6%	30%	41%	48%
	Use and somewhat ineffective	7%	4%	4%	13%	9%
	Don't Use	41%	79%	41%	20%	17%
	Don't Know	3%	6%	3%	1%	4%
Velocity of items deposited or paid	**Use and Very Effective**	11%	8%	13%	13%	8%
	Use and Somewhat effective	28%	19%	17%	38%	54%
	Use and somewhat ineffective	7%	6%	6%	8%	8%
	Don't Use	45%	52%	54%	38%	25%
	Don't Know	9%	15%	11%	5%	4%
Behavior analytics	**Use and Very Effective**	15%	15%	14%	15%	21%
	Use and Somewhat effective	25%	28%	23%	24%	29%
	Use and somewhat ineffective	4%	4%	1%	5%	13%
	Don't Use	47%	43%	51%	51%	33%
	Don't Know	8%	9%	11%	6%	4%
Positive and negative lists	**Use and Very Effective**	8%	8%	8%	12%	-
	Use and Somewhat effective	11%	10%	8%	11%	26%
	Use and somewhat ineffective	4%	10%	1%	5%	-
	Don't Use	66%	61%	76%	61%	57%
	Don't Know	10%	12%	6%	12%	17%
Shared database screen/score deposit items	**Use and Very Effective**	5%	4%	6%	3%	9%
	Use and Somewhat effective	10%	8%	9%	11%	17%
	Use and somewhat ineffective	1%	-	-	3%	-
	Don't Use	77%	80%	79%	79%	57%
	Don't Know	8%	8%	7%	5%	17%

Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate check remote deposit capture (RDC) fraud risks?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Limit on total RDC deposit value	**Use and Very Effective**	47%	45%	47%	48%	46%
	Use and Somewhat effective	35%	18%	40%	38%	25%
	Use and somewhat ineffective	6%	9%	2%	5%	17%
	Don't Use	9%	9%	9%	6%	13%
	Don't Know	3%	18%	2%	3%	-
Limit on RDS per item value	**Use and Very Effective**	41%	55%	42%	38%	42%
	Use and Somewhat effective	36%	18%	38%	38%	29%
	Use and somewhat ineffective	6%	9%	2%	5%	17%
	Don't Use	14%	9%	15%	15%	13%
	Don't Know	3%	9%	2%	3%	-
Limit on number of RDC items deposited	**Use and Very Effective**	29%	36%	31%	29%	21%
	Use and Somewhat effective	35%	9%	35%	43%	25%
	Use and somewhat ineffective	4%	-	-	6%	8%
	Don't Use	28%	36%	27%	19%	46%
	Don't Know	5%	18%	6%	3%	-
Velocity checks on RDC items	**Use and Very Effective**	23%	18%	28%	26%	4%
	Use and Somewhat effective	26%	36%	14%	26%	46%
	Use and somewhat ineffective	5%	9%	4%	3%	13%
	Don't Use	36%	18%	40%	38%	33%
	Don't Know	10%	18%	14%	7%	4%
IP address verification	**Use and Very Effective**	18%	9%	16%	24%	13%
	Use and Somewhat effective	17%	18%	16%	19%	13%
	Use and somewhat ineffective	5%	-	-	8%	8%
	Don't Use	48%	45%	53%	37%	67%
	Don't Know	12%	27%	16%	11%	-
Apply same screens/scoring methods as used in non-RDC check deposits	**Use and Very Effective**	14%	18%	18%	11%	8%
	Use and Somewhat effective	18%	18%	6%	23%	33%
	Use and somewhat ineffective	4%	9%	4%	5%	-
	Don't Use	46%	27%	49%	44%	54%
	Don't Know	18%	27%	24%	16%	4%
Device finger printing	**Use and Very Effective**	5%	-	10%	3%	-
	Use and Somewhat effective	8%	-	4%	7%	21%
	Use and somewhat ineffective	4%	-	2%	5%	8%
	Don't Use	76%	100%	73%	78%	67%
	Don't Know	8%	-	12%	7%	4%

Which of the following reporting and other risk management methods does your financial institution use to mitigate check fraud risks?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Provide staff education and training on check fraud risk mitigation	**Use and Very Effective**	27%	34%	26%	28%	13%
	Use and Somewhat effective	60%	41%	61%	67%	79%
	Use and somewhat ineffective	7%	13%	4%	6%	8%
	Don't Use	4%	5%	7%	-	-
	Don't Know	3%	7%	3%	-	-
Apply exception holds on funds availability	**Use and Very Effective**	50%	50%	46%	54%	54%
	Use and Somewhat effective	35%	25%	42%	36%	38%
	Use and somewhat ineffective	8%	9%	7%	7%	8%
	Don't Use	5%	13%	4%	3%	-
	Don't Know	1%	4%	1%	-	-
Provide customers online information services to view check images, statements, etc.	**Use and Very Effective**	46%	37%	46%	53%	46%
	Use and Somewhat effective	37%	28%	45%	37%	38%
	Use and somewhat ineffective	7%	9%	4%	4%	17%
	Don't Use	9%	25%	4%	6%	-
	Don't Know	1%	2%	1%	-	-
Routinely apply standard check holds on funds availability	**Use and Very Effective**	40%	52%	26%	41%	50%
	Use and Somewhat effective	33%	28%	42%	30%	33%
	Use and somewhat ineffective	11%	7%	14%	11%	8%
	Don't Use	15%	10%	18%	18%	8%
	Don't Know	1%	3%	1%	-	-
Monitor customer return item rates	**Use and Very Effective**	27%	39%	27%	20%	17%
	Use and Somewhat effective	37%	25%	35%	47%	42%
	Use and somewhat ineffective	12%	18%	7%	13%	8%
	Don't Use	20%	16%	26%	14%	33%
	Don't Know	4%	4%	5%	6%	-
Provide customer education and training on check fraud risk mitigation	**Use and Very Effective**	10%	9%	11%	12%	4%
	Use and Somewhat effective	33%	24%	26%	47%	33%
	Use and somewhat ineffective	27%	26%	23%	31%	33%
	Don't Use	25%	35%	33%	9%	25%
	Don't Know	5%	6%	7%	1%	4%
Provide customers alerts via text, email, or within application	**Use and Very Effective**	25%	21%	17%	35%	33%
	Use and Somewhat effective	25%	6%	31%	35%	21%
	Use and somewhat ineffective	9%	8%	13%	6%	13%
	Don't Use	37%	58%	37%	24%	25%
	Don't Know	4%	8%	3%	-	8%
Prohibit customer/payee from creating and depositing remotely created checks	**Use and Very Effective**	12%	21%	10%	10%	-
	Use and Somewhat effective	12%	4%	13%	13%	21%
	Use and somewhat ineffective	6%	2%	3%	7%	17%
	Don't Use	61%	62%	63%	58%	58%
	Don't Know	11%	11%	13%	10%	4%
Submit data to shared database and receive alerts	**Use and Very Effective**	6%	6%	4%	6%	13%
	Use and Somewhat effective	10%	8%	9%	12%	17%
	Use and somewhat ineffective	3%	4%	4%	1%	4%
	Don't Use	72%	69%	76%	75%	63%
	Don't Know	8%	13%	7%	6%	4%

What are the three current fraud attacks most often used to initiate ACH fraud against your financial institution or your customer's accounts?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Fraudulent or unauthorized ACH debits against consumer accounts	**1st Choice**	81%	89%	80%	78%	79%
	2nd Choice	10%	5%	12%	10%	13%
	3rd Choice	2%	-	2%	1%	4%
Fraudulent or unauthorized ACH debits against business accounts	**1st Choice**	6%	-	8%	6%	8%
	2nd Choice	42%	26%	38%	49%	54%
	3rd Choice	9%	3%	12%	10%	4%
Use of fraudulent credentials or other data to defraud existing accounts	**1st Choice**	3%	3%	3%	3%	-
	2nd Choice	9%	11%	9%	7%	8%
	3rd Choice	15%	16%	15%	16%	8%
Identity theft or synthetic identity theft used to defraud existing accounts	**1st Choice**	2%	3%	3%	-	-
	2nd Choice	8%	13%	9%	6%	4%
	3rd Choice	12%	11%	9%	10%	25%
Account takeover of customers' accounts	**1st Choice**	3%	3%	2%	4%	4%
	2nd Choice	6%	8%	3%	6%	8%
	3rd Choice	11%	3%	5%	13%	33%
Business email compromise schemes	**1st Choice**	3%	-	-	6%	8%
	2nd Choice	4%	3%	2%	7%	8%
	3rd Choice	9%	-	5%	16%	13%
Abuse of power of attorney to defraud vulnerable adult	**1st Choice**	1%	-	2%	1%	-
	2nd Choice	4%	5%	6%	3%	-
	3rd Choice	7%	8%	8%	7%	4%
Originator company employee frauds, e.g., payroll, invoice payment	**1st Choice**	1%	-	2%	-	-
	2nd Choice	3%	5%	2%	3%	4%
	3rd Choice	2%	-	3%	3%	-
Insider fraud	**1st Choice**	1%	-	-	1%	-
	2nd Choice	1%	-	-	3%	-
	3rd Choice	1%	5%	-	-	-

Which of the following ACH originator/sender authentication methods does your financial institution use to mitigate ACH fraud risks?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
ID and Password for consumer billpay	**Use and Very Effective**	58%	66%	54%	69%	30%
	Use and Somewhat effective	31%	10%	35%	26%	57%
	Use and somewhat ineffective	2%	-	3%	1%	4%
	Don't Use	7%	17%	8%	3%	4%
	Don't Know	2%	7%	-	-	4%
Multi-factor authentication for consumer billpay	**Use and Very Effective**	46%	55%	43%	51%	27%
	Use and Somewhat effective	29%	17%	40%	24%	27%
	Use and somewhat ineffective	3%	3%	2%	1%	14%
	Don't Use	19%	17%	14%	22%	27%
	Don't Know	3%	7%	2%	1%	5%
Multi-factor authentication with originating company/third party sender	**Use and Very Effective**	47%	40%	33%	57%	64%
	Use and Somewhat effective	22%	8%	27%	20%	27%
	Use and somewhat ineffective	2%	4%	4%	-	5%
	Don't Use	21%	28%	29%	17%	5%
	Don't Know	8%	20%	7%	7%	-
Dual control for originating company file initiation	**Use and Very Effective**	43%	44%	39%	47%	45%
	Use and Somewhat effective	25%	7%	25%	31%	32%
	Use and somewhat ineffective	2%	-	4%	2%	-
	Don't Use	21%	22%	25%	18%	23%
	Don't Know	8%	26%	9%	3%	-
Evaluate new credential requests for originator before issuing	**Use and Very Effective**	35%	22%	36%	45%	29%
	Use and Somewhat effective	24%	11%	30%	24%	38%
	Use and somewhat ineffective	2%	2%	3%	2%	4%
	Don't Use	29%	43%	26%	20%	29%
	Don't Know	10%	22%	5%	9%	-
Out-of-band authentication with originating company/third party sender	**Use and Very Effective**	30%	8%	31%	33%	50%
	Use and Somewhat effective	17%	23%	11%	13%	36%
	Use and somewhat ineffective	1%	-	2%	-	5%
	Don't Use	37%	35%	45%	41%	9%
	Don't Know	14%	35%	11%	13%	-
IP address verification	**Use and Very Effective**	19%	9%	15%	25%	38%
	Use and Somewhat effective	17%	7%	20%	22%	21%
	Use and somewhat ineffective	5%	5%	5%	6%	4%
	Don't Use	43%	49%	47%	37%	38%
	Don't Know	15%	29%	14%	11%	-

Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate ACH fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
OFAC monitoring	**Use and Very Effective**	46%	52%	41%	45%	50%
	Use and Somewhat effective	40%	29%	43%	43%	46%
	Use and somewhat ineffective	10%	10%	16%	4%	4%
	Don't Use	2%	5%	-	3%	-
	Don't Know	2%	3%	-	4%	-
Manual review	**Use and Very Effective**	40%	49%	42%	33%	33%
	Use and Somewhat effective	37%	27%	42%	42%	25%
	Use and somewhat ineffective	6%	5%	3%	6%	17%
	Don't Use	11%	9%	7%	12%	25%
	Don't Know	6%	9%	6%	6%	-
Transaction value	**Use and Very Effective**	26%	19%	28%	31%	29%
	Use and Somewhat effective	34%	15%	39%	38%	54%
	Use and somewhat ineffective	6%	7%	7%	5%	4%
	Don't Use	24%	37%	19%	22%	13%
	Don't Know	9%	22%	7%	5%	-
Out of pattern activity	**Use and Very Effective**	29%	25%	29%	34%	25%
	Use and Somewhat effective	31%	23%	34%	30%	42%
	Use and somewhat ineffective	4%	5%	3%	4%	-
	Don't Use	28%	26%	27%	28%	33%
	Don't Know	9%	21%	7%	3%	-
Suspend originated files exceeding exposure limits	**Use and Very Effective**	25%	8%	27%	30%	46%
	Use and Somewhat effective	24%	14%	22%	38%	17%
	Use and somewhat ineffective	3%	8%	1%	-	4%
	Don't Use	33%	41%	34%	25%	33%
	Don't Know	14%	29%	15%	6%	-
Anomaly/behavior analytics	**Use and Very Effective**	20%	13%	18%	22%	35%
	Use and Somewhat effective	22%	19%	21%	22%	30%
	Use and somewhat ineffective	4%	2%	6%	3%	9%
	Don't Use	39%	35%	41%	46%	26%
	Don't Know	15%	31%	15%	6%	-
Velocity of ACH transactions	**Use and Very Effective**	16%	11%	19%	17%	13%
	Use and Somewhat effective	25%	11%	18%	33%	58%
	Use and somewhat ineffective	4%	6%	4%	2%	4%
	Don't Use	40%	46%	40%	41%	21%
	Don't Know	15%	26%	19%	6%	4%
Rules based fraud detection	**Use and Very Effective**	14%	8%	13%	17%	21%
	Use and Somewhat effective	24%	10%	25%	27%	42%
	Use and somewhat ineffective	5%	8%	3%	6%	4%
	Don't Use	43%	42%	48%	42%	29%
	Don't Know	14%	33%	10%	8%	4%
ACH block services	**Use and Very Effective**	12%	11%	6%	13%	25%
	Use and Somewhat effective	20%	20%	17%	18%	33%
	Use and somewhat ineffective	3%	6%	-	2%	8%
	Don't Use	51%	35%	70%	54%	29%
	Don't Know	15%	28%	8%	13%	4%
ACH filter/positive pay services	**Use and Very Effective**	9%	10%	3%	7%	29%
	Use and Somewhat effective	16%	10%	9%	20%	38%
	Use and somewhat ineffective	3%	4%	2%	5%	4%
	Don't Use	55%	39%	74%	59%	25%
	Don't Know	17%	37%	12%	10%	4%
Shared database screen/score deposit items	**Use and Very Effective**	5%	6%	7%	5%	-
	Use and Somewhat effective	6%	8%	6%	5%	8%
	Use and somewhat ineffective	1%	-	1%	2%	4%
	Don't Use	71%	57%	72%	78%	79%
	Don't Know	16%	30%	13%	11%	8%

Which of the following reporting and other risk management methods does your financial institution use to mitigate ACH fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Provide customers online information services to view transactions, statements, etc.	**Use and Very Effective**	50%	48%	45%	55%	50%
	Use and Somewhat effective	37%	17%	48%	37%	42%
	Use and somewhat ineffective	4%	4%	4%	4%	4%
	Don't Use	7%	21%	3%	1%	4%
	Don't Know	3%	10%	-	1%	-
Provide staff education and training on ACH fraud risk mitigation	**Use and Very Effective**	29%	35%	26%	29%	25%
	Use and Somewhat effective	53%	33%	56%	63%	58%
	Use and somewhat ineffective	8%	6%	10%	4%	17%
	Don't Use	7%	16%	8%	-	-
	Don't Know	3%	10%	-	3%	-
Limit ACH origination to domestic transactions	**Use and Very Effective**	50%	48%	48%	52%	50%
	Use and Somewhat effective	28%	7%	33%	33%	27%
	Use and somewhat ineffective	1%	-	4%	-	-
	Don't Use	17%	33%	11%	12%	23%
	Don't Know	4%	11%	4%	3%	-
Monitor customer return item rates	**Use and Very Effective**	26%	29%	19%	34%	17%
	Use and Somewhat effective	39%	21%	45%	42%	58%
	Use and somewhat ineffective	8%	11%	9%	4%	13%
	Don't Use	18%	25%	21%	12%	8%
	Don't Know	8%	14%	6%	7%	4%
Provide customer education and training on ACH fraud risk mitigation	**Use and Very Effective**	15%	13%	16%	13%	21%
	Use and Somewhat effective	35%	21%	31%	52%	29%
	Use and somewhat ineffective	24%	17%	24%	22%	42%
	Don't Use	22%	38%	28%	10%	4%
	Don't Know	5%	13%	1%	3%	4%
Provide customers alerts via text, email, or within application	**Use and Very Effective**	24%	16%	21%	30%	33%
	Use and Somewhat effective	19%	2%	25%	22%	29%
	Use and somewhat ineffective	8%	6%	6%	9%	13%
	Don't Use	41%	64%	43%	28%	25%
	Don't Know	8%	12%	6%	11%	-
Originator services to establish batch-level thresholds to hold batches for added authorizations	**Use and Very Effective**	22%	12%	28%	23%	25%
	Use and Somewhat effective	25%	10%	16%	41%	38%
	Use and somewhat ineffective	4%	4%	3%	5%	4%
	Don't Use	40%	54%	48%	23%	33%
	Don't Know	9%	20%	6%	8%	-
Provide account masking services	**Use and Very Effective**	19%	12%	21%	21%	26%
	Use and Somewhat effective	23%	10%	24%	32%	22%
	Use and somewhat ineffective	5%	2%	6%	5%	13%
	Don't Use	38%	50%	38%	29%	35%
	Don't Know	15%	26%	12%	13%	4%
Funds availability delay when reasonably suspect ACH credit received is unauthorized	**Use and Very Effective**	15%	16%	21%	13%	4%
	Use and Somewhat effective	24%	27%	24%	23%	25%
	Use and somewhat ineffective	7%	2%	6%	8%	17%
	Don't Use	38%	37%	34%	40%	42%
	Don't Know	16%	18%	16%	16%	13%
Established procedures for identifying money mule accounts	**Use and Very Effective**	13%	16%	12%	11%	13%
	Use and Somewhat effective	21%	14%	21%	21%	42%
	Use and somewhat ineffective	9%	4%	7%	11%	17%
	Don't Use	41%	40%	49%	38%	29%
	Don't Know	16%	26%	12%	19%	-

Continued - Which of the following reporting and other risk management methods does your financial institution use to mitigate ACH fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Provide ACH originator alerts, e.g., notice of new payee added	**Use and Very Effective**	17%	10%	13%	22%	33%
	Use and Somewhat effective	20%	16%	18%	28%	13%
	Use and somewhat ineffective	5%	6%	1%	6%	13%
	Don't Use	48%	51%	60%	35%	42%
	Don't Know	10%	18%	7%	9%	-
Provide ACH receiver alerts, e.g., ACH debit alerts	**Use and Very Effective**	14%	14%	10%	20%	13%
	Use and Somewhat effective	20%	10%	16%	26%	33%
	Use and somewhat ineffective	6%	-	3%	11%	17%
	Don't Use	46%	53%	60%	30%	38%
	Don't Know	13%	24%	10%	14%	-
Outsource ACH processing and risk management	**Use and Very Effective**	11%	22%	8%	7%	8%
	Use and Somewhat effective	13%	18%	15%	7%	8%
	Use and somewhat ineffective	2%	-	-	3%	4%
	Don't Use	67%	45%	74%	72%	79%
	Don't Know	8%	14%	3%	12%	-
Provide customers online services to dispute transactions	**Use and Very Effective**	8%	10%	7%	8%	4%
	Use and Somewhat effective	6%	2%	4%	8%	17%
	Use and somewhat ineffective	2%	-	1%	3%	4%
	Don't Use	79%	78%	84%	78%	71%
	Don't Know	5%	10%	3%	3%	4%

What are the three current fraud attacks most often used to initiate wire fraud against your financial institution or your customer's accounts?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Business email compromise schemes	**1st Choice**	36%	-	24%	45%	74%
	2nd Choice	14%	-	15%	18%	13%
	3rd Choice	5%	5%	6%	4%	4%
Consumer victim frauds	**1st Choice**	28%	32%	35%	21%	22%
	2nd Choice	16%	11%	9%	21%	22%
	3rd Choice	9%	-	2%	13%	22%
Use of fraudulent credentials or other data to defraud existing accounts	**1st Choice**	7%	5%	9%	7%	-
	2nd Choice	14%	26%	11%	11%	17%
	3rd Choice	11%	-	4%	18%	17%
Account takeover of customers' accounts	**1st Choice**	9%	5%	6%	14%	4%
	2nd Choice	9%	11%	4%	7%	26%
	3rd Choice	11%	11%	6%	13%	22%
Identity theft or synthetic identity theft used to defraud existing accounts	**1st Choice**	3%	11%	2%	4%	-
	2nd Choice	10%	5%	9%	11%	13%
	3rd Choice	13%	21%	9%	14%	9%
Originator company employee frauds	**1st Choice**	3%	11%	2%	2%	-
	2nd Choice	4%	5%	-	7%	4%
	3rd Choice	5%	11%	6%	-	9%
Abuse of power of attorney to defraud vulnerable adult	**1st Choice**	1%	5%	2%	-	-
	2nd Choice	7%	5%	7%	9%	-
	3rd Choice	3%	5%	4%	4%	-
Insider fraud	**1st Choice**	2%	-	2%	4%	-
	2nd Choice	2%	5%	2%	-	4%
	3rd Choice	3%	5%	2%	5%	-

Which of the following transaction authentication methods does your financial institution use to mitigate wire fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Telephone callback verification	**Use and Very Effective**	70%	56%	66%	85%	63%
	Use and Somewhat effective	18%	19%	21%	12%	25%
	Use and somewhat ineffective	2%	5%	-	-	8%
	Don't Use	9%	14%	14%	3%	4%
	Don't Know	1%	7%	-	-	-
Signature verification	**Use and Very Effective**	55%	59%	57%	58%	33%
	Use and Somewhat effective	26%	20%	33%	27%	17%
	Use and somewhat ineffective	8%	5%	6%	7%	21%
	Don't Use	8%	10%	4%	6%	25%
	Don't Know	2%	7%	-	1%	4%
Dual control for originating company wire initiation	**Use and Very Effective**	57%	67%	51%	60%	54%
	Use and Somewhat effective	20%	17%	20%	20%	29%
	Use and somewhat ineffective	3%	2%	3%	2%	13%
	Don't Use	16%	7%	25%	17%	-
	Don't Know	3%	7%	1%	2%	4%
Evaluate new credential requests for originator before issuing	**Use and Very Effective**	34%	33%	30%	41%	30%
	Use and Somewhat effective	26%	20%	25%	29%	35%
	Use and somewhat ineffective	2%	5%	2%	-	4%
	Don't Use	29%	25%	39%	24%	22%
	Don't Know	8%	18%	5%	6%	9%
Limit consumer initiated wires to in person requests with valid government issued ID	**Use and Very Effective**	42%	50%	39%	44%	29%
	Use and Somewhat effective	11%	12%	12%	13%	4%
	Use and somewhat ineffective	2%	2%	1%	2%	4%
	Don't Use	44%	31%	48%	40%	63%
	Don't Know	2%	5%	-	2%	-
Multi-factor authentication with originating company	**Use and Very Effective**	37%	38%	21%	44%	58%
	Use and Somewhat effective	14%	15%	8%	17%	17%
	Use and somewhat ineffective	1%	3%	-	2%	-
	Don't Use	44%	33%	68%	36%	21%
	Don't Know	4%	10%	3%	2%	4%
Out-of-band authentication with originating company	**Use and Very Effective**	24%	30%	11%	22%	54%
	Use and Somewhat effective	12%	8%	10%	16%	17%
	Use and somewhat ineffective	2%	-	-	5%	-
	Don't Use	53%	48%	70%	51%	21%
	Don't Know	9%	15%	10%	6%	8%
IP address verification	**Use and Very Effective**	12%	8%	11%	14%	17%
	Use and Somewhat effective	9%	5%	6%	11%	21%
	Use and somewhat ineffective	4%	-	-	6%	13%
	Don't Use	66%	75%	78%	57%	46%
	Don't Know	8%	13%	5%	11%	4%
Device finger printing	**Use and Very Effective**	2%	-	3%	2%	-
	Use and Somewhat effective	2%	-	3%	2%	-
	Use and somewhat ineffective	2%	-	-	3%	8%
	Don't Use	90%	90%	91%	90%	88%
	Don't Know	5%	10%	3%	3%	4%

Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate wire fraud risks?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
OFAC monitoring	**Use and Very Effective**	47%	51%	42%	45%	58%
	Use and Somewhat effective	38%	29%	44%	38%	38%
	Use and somewhat ineffective	10%	11%	11%	9%	4%
	Don't Use	2%	2%	3%	3%	-
	Don't Know	3%	7%	-	5%	-
Manual review	**Use and Very Effective**	63%	71%	67%	59%	48%
	Use and Somewhat effective	27%	16%	27%	35%	30%
	Use and somewhat ineffective	3%	2%	3%	-	17%
	Don't Use	4%	4%	4%	3%	4%
	Don't Know	2%	7%	-	3%	-
Transaction value	**Use and Very Effective**	33%	41%	34%	28%	26%
	Use and Somewhat effective	37%	23%	36%	44%	48%
	Use and somewhat ineffective	8%	10%	6%	8%	13%
	Don't Use	18%	21%	20%	16%	13%
	Don't Know	4%	5%	4%	5%	-
Out of pattern activity	**Use and Very Effective**	38%	42%	42%	32%	35%
	Use and Somewhat effective	32%	23%	27%	45%	26%
	Use and somewhat ineffective	7%	5%	7%	6%	17%
	Don't Use	18%	21%	21%	14%	17%
	Don't Know	4%	9%	3%	3%	4%
Velocity of wire transactions	**Use and Very Effective**	20%	19%	25%	15%	17%
	Use and Somewhat effective	25%	17%	22%	28%	39%
	Use and somewhat ineffective	7%	7%	4%	10%	9%
	Don't Use	40%	48%	38%	40%	30%
	Don't Know	8%	10%	10%	7%	4%
Suspend originated wires exceeding exposure limits	**Use and Very Effective**	22%	26%	22%	13%	41%
	Use and Somewhat effective	25%	18%	18%	35%	27%
	Use and somewhat ineffective	4%	3%	-	8%	5%
	Don't Use	41%	39%	52%	38%	18%
	Don't Know	9%	13%	8%	6%	9%
Anomaly/behavior analytics	**Use and Very Effective**	23%	33%	25%	13%	30%
	Use and Somewhat effective	23%	15%	16%	29%	39%
	Use and somewhat ineffective	3%	-	3%	3%	9%
	Don't Use	45%	41%	50%	52%	17%
	Don't Know	6%	10%	6%	3%	4%
Rules based fraud detection	**Use and Very Effective**	16%	22%	15%	10%	26%
	Use and Somewhat effective	16%	24%	8%	18%	22%
	Use and somewhat ineffective	5%	-	5%	2%	22%
	Don't Use	53%	44%	64%	61%	22%
	Don't Know	9%	10%	9%	10%	9%

Which of the following reporting and other risk management methods does your financial institution use to mitigate wire fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Provide staff education and training on wire fraud risk mitigation	**Use and Very Effective**	37%	51%	36%	32%	26%
	Use and Somewhat effective	51%	36%	47%	62%	65%
	Use and somewhat ineffective	6%	4%	8%	4%	9%
	Don't Use	3%	2%	7%	1%	-
	Don't Know	2%	7%	1%	-	-
Provide customers online information services to view transactions, statements, etc.	**Use and Very Effective**	54%	60%	52%	55%	50%
	Use and Somewhat effective	34%	12%	40%	40%	42%
	Use and somewhat ineffective	5%	5%	5%	4%	4%
	Don't Use	5%	17%	3%	-	4%
	Don't Know	1%	7%	-	-	-
Refuse to send consumer initiated wire when suspect fraud scheme	**Use and Very Effective**	61%	60%	52%	69%	67%
	Use and Somewhat effective	20%	7%	30%	19%	17%
	Use and somewhat ineffective	7%	5%	4%	9%	17%
	Don't Use	7%	14%	8%	3%	-
	Don't Know	5%	14%	5%	-	-
Provide customer education and training on wire fraud risk mitigation	**Use and Very Effective**	12%	7%	15%	12%	13%
	Use and Somewhat effective	33%	31%	19%	51%	29%
	Use and somewhat ineffective	22%	17%	24%	20%	33%
	Don't Use	27%	38%	33%	17%	17%
	Don't Know	6%	7%	9%	-	8%
Funds availability delay when reasonably suspect wire received is unauthorized	**Use and Very Effective**	32%	41%	31%	32%	21%
	Use and Somewhat effective	28%	12%	28%	36%	33%
	Use and somewhat ineffective	6%	5%	4%	3%	21%
	Don't Use	25%	29%	28%	21%	17%
	Don't Know	9%	12%	9%	8%	8%
Complete standard list of questions with consumer initiated wires	**Use and Very Effective**	30%	33%	29%	29%	29%
	Use and Somewhat effective	24%	16%	23%	31%	25%
	Use and somewhat ineffective	11%	9%	9%	10%	21%
	Don't Use	31%	35%	35%	29%	21%
	Don't Know	4%	7%	4%	2%	4%
Provide recurring wire templates to originators with role based security for changes	**Use and Very Effective**	23%	22%	17%	26%	33%
	Use and Somewhat effective	28%	22%	21%	39%	33%
	Use and somewhat ineffective	6%	7%	3%	6%	8%
	Don't Use	39%	41%	53%	27%	25%
	Don't Know	4%	7%	6%	2%	-
Provide customers alerts via text, email, or within application	**Use and Very Effective**	21%	24%	16%	25%	21%
	Use and Somewhat effective	23%	-	26%	33%	29%
	Use and somewhat ineffective	7%	2%	6%	8%	17%
	Don't Use	45%	66%	49%	32%	33%
	Don't Know	3%	7%	3%	2%	-
Established procedures for identifying money mule accounts	**Use and Very Effective**	13%	20%	11%	16%	4%
	Use and Somewhat effective	24%	17%	20%	25%	46%
	Use and somewhat ineffective	5%	-	5%	5%	17%
	Don't Use	46%	44%	56%	42%	33%
	Don't Know	11%	20%	9%	13%	-

Continued - Which of the following reporting and other risk management methods does your financial institution use to mitigate wire fraud risks?

			Respondent Size - Total Assets in Millions of Dollars			
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Limit wire origination to domestic transactions	**Use and Very Effective**	24%	48%	23%	18%	-
	Use and Somewhat effective	14%	7%	20%	11%	17%
	Use and somewhat ineffective	1%	-	1%	-	4%
	Don't Use	58%	39%	55%	69%	75%
	Don't Know	3%	7%	-	2%	4%
Provide customers online services to dispute transactions	**Use and Very Effective**	8%	10%	4%	11%	4%
	Use and Somewhat effective	6%	2%	6%	6%	13%
	Use and somewhat ineffective	2%	-	-	2%	8%
	Don't Use	82%	78%	90%	80%	71%
	Don't Know	3%	10%	-	2%	4%
Outsource wire processing and risk management	**Use and Very Effective**	6%	17%	7%	-	-
	Use and Somewhat effective	5%	17%	3%	2%	-
	Use and somewhat ineffective	1%	2%	-	2%	-
	Don't Use	84%	54%	88%	94%	96%
	Don't Know	4%	10%	1%	3%	4%

Which of the following internal controls and procedures does your financial institution use to mitigate fraud risks?

		Respondent Size - Total Assets in Millions of Dollars				
		Overall	**Less than $50**	**$50 - $199.9**	**$200 - $999.9**	**$1000+**
Address exception items timely, e.g., meet deadlines for chargebacks, returning payments, etc.	**Use and Very Effective**	62%	66%	60%	60%	63%
	Use and Somewhat effective	28%	15%	31%	35%	25%
	Use and somewhat ineffective	3%	4%	3%	1%	8%
	Don't Use	4%	6%	5%	1%	-
	Don't Know	4%	9%	1%	1%	4%
Dual controls and segregation of duties within payment initiation and receipt processes	**Use and Very Effective**	70%	59%	67%	82%	71%
	Use and Somewhat effective	20%	18%	25%	15%	25%
	Use and somewhat ineffective	-	-	1%	-	-
	Don't Use	7%	16%	7%	3%	-
	Don't Know	2%	7%	-	-	4%
Authentication and authorization controls to payment processes	**Use and Very Effective**	66%	65%	64%	69%	63%
	Use and Somewhat effective	22%	13%	26%	21%	33%
	Use and somewhat ineffective	2%	2%	3%	3%	-
	Don't Use	4%	7%	4%	3%	-
	Don't Know	6%	13%	3%	4%	4%
Transaction/file approval limits	**Use and Very Effective**	58%	53%	55%	66%	58%
	Use and Somewhat effective	28%	25%	32%	25%	25%
	Use and somewhat ineffective	3%	-	4%	3%	8%
	Don't Use	8%	15%	7%	4%	4%
	Don't Know	3%	8%	1%	1%	4%
Physical access controls to payment processing functions	**Use and Very Effective**	59%	62%	57%	59%	54%
	Use and Somewhat effective	28%	21%	26%	35%	33%
	Use and somewhat ineffective	1%	-	4%	-	-
	Don't Use	8%	8%	12%	3%	8%
	Don't Know	4%	9%	1%	3%	4%
Logical access controls to your computing network and payment processing applications	**Use and Very Effective**	64%	52%	67%	72%	63%
	Use and Somewhat effective	21%	13%	26%	18%	33%
	Use and somewhat ineffective	-	2%	-	-	-
	Don't Use	9%	21%	5%	6%	-
	Don't Know	5%	12%	1%	4%	4%
Restrict or limit employee use of Internet from financial institution's network	**Use and Very Effective**	42%	43%	38%	46%	38%
	Use and Somewhat effective	32%	32%	35%	28%	33%
	Use and somewhat ineffective	10%	2%	8%	16%	17%
	Don't Use	13%	16%	18%	9%	4%
	Don't Know	3%	7%	1%	-	8%
Prohibit use of personal devices for processing of financial institution's payment transactions	**Use and Very Effective**	65%	56%	69%	69%	63%
	Use and Somewhat effective	17%	9%	20%	16%	25%
	Use and somewhat ineffective	1%	4%	1%	-	-
	Don't Use	12%	22%	8%	12%	4%
	Don't Know	5%	9%	1%	3%	8%
Dedicated computer used to conduct transactions with payments network operator, correspondent bank, or financial service provider	**Use and Very Effective**	26%	23%	28%	28%	21%
	Use and Somewhat effective	13%	10%	11%	15%	17%
	Use and somewhat ineffective	2%	4%	-	-	8%
	Don't Use	54%	54%	60%	54%	42%
	Don't Know	5%	10%	1%	3%	13%