Financial Technology and Innovation

♦ ISSN: 2836-5372 Vol: 04, No. 02, 2024 ♦ PP. 01–08
Article DOI: https://doi.org/10.54216/FinTech-I.040201

FULL LENGTH ARTICLE

The Fraud-Protection Paradox in Consumer Payments

Taif Khalid Shakir[1] **Ahmed N. Al Masri**[2,*]

[1] Ascencia Business School, College de Paris, France
[2] Department of Studies, Research and Development, Ministry of Energy and Infrastructure, Abu Dhabi 11191, United Arab Emirates
Emails: taif.shakir@cabling.att-mail.com · ahmed.almasri32@gmail.com
Received: January 03, 2024 Revised: March 01, 2024 Accepted: June 05, 2024 ⋆ Corresponding author

ABSTRACT

Consumer-payment risk is hard to measure because instruments that have the highest incidence of reported fraud are often still in high usage and trusted. The key debate is when to break down the line between weak security and a protection ecosystem that will minimise the impact consumers suffer following an incident, through monitoring, liability allocation, dispute handling and recovery. This paper constructs a framework for risk alignment between instrument-level fraud incidence, perceived security, and realized payment use, and breaks down the difference between persistent instrument-level differences and short-run changes within instruments. Official U.S. estimates for cash, checks, debit cards, and credit cards are arranged in a balanced panel for the years 2015-2020 and an extended descriptive sample for 2022. Combined results of pooled regression, two-way fixed effects, first differences, and leave-one-year-out ridge validation to ascertain if fraud exposure can be predicted after accounting for stable instrument characteristics and common annual shocks. Regulators and payment providers need to address this measurement challenge since a narrow focus on incident counts can divert investment focus from detection, liability limits, recovery, and reimbursement capabilities that build consumer confidence and payment-system robustness. Credit-card payment share rose from 18.3% in 2015 to 31.3% in 2022 while 10.3% of adopters reported loss, theft, or fraud in 2022; the pooled fraud coefficient of 3.86 ($p < .001$) fell to 2.20 ($p = .185$) under instrument and year fixed effects, and lagged fraud did not predict annual share change (-0.27, $p = .401$). The validation using leave-one-year-out results in an $R^2 = .873$ and MAE of 2.90 percentage points, whereas the instrument-history validation produces an MAE of 2.71.

Keywords: Payment fraud ▪ Consumer payments ▪ FinTech ▪ Perceived security ▪ Payment choice ▪ Digital financial services

1. INTRODUCTION

Payment has evolved in both the instruments that consumers use and the infrastructure that enables transactions to be authorized, monitored and settled. The greater the surface area of a transaction, the more opportunities for loss, theft, and fraud. Cards, mobile interfaces, tokenized credentials and platform-based services increase transaction friction, but they also increase the surface area through which it can occur. A rule of thumb in the standard behavioral expectation is that an instrument that seems insecure will lose users and transaction share. Real payment behavior is not as straightforward. Despite reports of credit and debit card fraud, they continue to be the leading payment methods, and a number of low-fraud instruments are on the downside.

For financial tech, this discrepancy is significant since security is not perceived as a one-time possibility. Consumers can differentiate between the probability of an event happening and the impact that it will have on them. When the incidence of reported events is relatively high, an instrument may appear to feel protected through authentication, transaction notifications, dispute processes, liability allocation and reimbursement. On the other hand, an instrument might have low recorded fraud and be unattractive due to its lack of convenience, acceptance, speed, or recoverability. Payment choice is thus a combined measure of convenience, acceptability, control and recoverability, not prevention.

Previous studies have shown that convenience and transaction attributes are key factors in payment choice [1, 2, 3]; trust, perceived risk, and payment continuation in mobile payments [4, 5, 6]; and effects of payment technologies on spending and financial behavior generally [7, 8]. However, the study of perception and incident exposure and actual instrument use tends to be – often – studied separately. The separation creates difficulties in assessing whether the cross-instrument correlations are real or due to the differences in the instruments.

The paper asks three questions to fill that gap. First of all, what is the correlation between the perception of security, reported fraud incidence, and payment shares for key payment instruments? Second, does the incidence of fraud explain the payment share once instrument differences (which are stable across the years) and common year effects are removed? Third, can risk and perception variables outperform just a simple instrument-history benchmark in predicting out of year? The analysis helps in distinguishing between pooled composition and within-instrument change, provides a common-year risk-alignment comparison, and provides a test of predictive value in a clear baseline. The findings show a paradox: despite having the highest level of perception about security and a growing share of the populace using them, credit cards have relatively high numbers of reports of incident exposure. This is not proof that fraud leads to usage. It shows that the frequency of the incidents is not the only measure of the consumer protection that is associated with a payment instrument.

The remainder of the paper is organized as follows. Section 2 reviews research on payment choice, trust, security, and FinTech risk allocation. Section 3 describes the data, variable construction, econometric specifications, predictive validation, and analytical workflow. Section 4 reports the descriptive, inferential, and out-of-year results. Section 5 discusses the protection mechanism and its implications for providers, regulators, and researchers. Section 6 states the study limitations, and Section 7 concludes.

2. RELATED WORK

2.1 Payment choice and transaction attributes

Payment instruments differ in speed, acceptance, record keeping, liquidity effects, and transaction salience. Electronic-payment convenience can reduce cash demand, although the strength of substitution varies across consumers and contexts [1]. Low-income households also face distinctive constraints that affect payment choice and access [2]. Experimental and behavioral studies show that payment interfaces can influence willingness to pay and spending intensity, reinforcing the view that the instrument is part of the consumption decision rather than a neutral settlement mechanism [3, 7, 8].

Mobile-payment research extends this argument by emphasizing usefulness, ease of use, acceptance, and habit. Merchant readiness and ecosystem support can enable or obstruct adoption [6], while switching from cash depends on more than technical availability [5]. Cross-country evidence similarly shows that adoption drivers are conditioned by institutional and market context [9, 10]. Studies conducted during the pandemic highlight perceived severity and self-efficacy as additional determinants [11], and evidence from China links mobile-payment use with access to conventional banking services [12].

2.2 Trust, security, and continuity

Trust and risk have been treated primarily as antecedents of adoption intention. Initial trust is important not only at first use but also for continuation [4]. Reviews of digital-payment adoption likewise identify perceived security and trust as recurring constructs, while noting fragmented operationalization across studies [13]. Research on open banking reaches a similar conclusion: consumers evaluate the institution, technology, data practice, and service proposition jointly rather than responding to openness in isolation [14].

This literature provides strong evidence that security beliefs matter, but it offers less evidence on how those beliefs relate to instrument-level incident experience over time. A highly protected instrument may record more incidents simply because it is used more often, accepted more widely, and monitored more intensively. It may also retain demand because liability and dispute mechanisms reduce the expected burden borne by the user. Distinguishing these mechanisms requires an analysis that separates cross-instrument levels from within-instrument changes.

2.3 FinTech governance and risk allocation

The governance literature places payment security within the wider transformation of financial intermediation. FinTech changes the organization of banking services, data access, and competition [15, 16]. Platformization can redistribute control among banks, payment firms, technology providers, and consumers, making liability and consumer interest central design questions [17]. Digital capability may improve inclusion and service access [18], but it also introduces new forms of credit, operational, and conduct risk [19]. Open-data arrangements further show that ownership and portability can intensify competition while making governance quality decisive [20]. Household adoption remains heterogeneous even where technologies are broadly available [21].

Table 1 summarizes representative streams and clarifies the present paper's position. Rather than estimating another intention model or transaction-level fraud detector, the study evaluates whether aggregate security perceptions and experienced incidents explain the evolving use of established payment instruments.

3. DATA AND METHODS

3.1 Data source and analytical scope

The analysis draws on annual estimates from the Federal Reserve Bank of Atlanta's Survey and Diary of Consumer Payment Choice [22]. The source combines consumer re-

Table 1. Representative research streams and the gap addressed in this study.

Reference	Focus	Evidence	Main implication	Unresolved issue addressed here
[1]	Electronic-payment convenience and cash demand	Consumer payment behavior	Convenience can accelerate substitution away from cash.	Does experienced risk alter the trajectory after instrument differences are controlled?
[3]	Credit-card versus mobile-payment effects	Behavioral experiment	Payment interfaces influence convenience and willingness to pay.	Interface effects do not reveal whether incident exposure changes market share.
[4]	Trust and mobile-payment continuation	Survey modeling	Initial trust remains relevant beyond adoption.	Trust constructs are not aligned with observed instrument-level fraud and use.
[5]	Barriers to switching from cash	Consumer survey	Switching depends on utility, resistance, and context.	The role of measured incident exposure in continued use remains unclear.
[13]	Digital-payment adoption literature	Structured literature review	Security and trust recur across adoption frameworks.	Comparative longitudinal evidence remains limited.
[17]	Platformization and consumer interest	Legal and policy analysis	Payment platforms redistribute power and responsibility.	Aggregate evidence is needed on whether protection and incident rates align.
[15]	FinTech and banking transformation	Finance review	Technology changes intermediation without eliminating core financial functions.	Consumer-payment protection requires a measure beyond technology adoption.
Present study	Fraud, protection, and instrument use	Official annual estimates; pooled, fixed-effects, first-difference, and predictive models	Prevention, perceived security, and use need not move together.	Separates between-instrument composition from within-instrument response and benchmarks predictive value.

ports about payment-instrument characteristics and adverse experiences with diary-based estimates of payment activity. The study uses observations from 2015 through 2022 for cash, checks, debit cards, and credit cards. No observation or source released after March 2024 is included.

Let $\mathscr{I} = \{\text{cash, check, debit, credit}\}$ denote the instrument set and let $\mathscr{T} = \{2015,\dots,2022\}$. The observed panel is

$$\mathscr{D} = \{(S_{it}, F_{it}, R_{it}) : i \in \mathscr{I},\ t \in \mathscr{T}\}, \tag{1}$$

where S_{it} is payment share, F_{it} is fraud incidence, and R_{it} is perceived-security rank. The analytical table contains 30 instrument–year observations. A questionnaire comparability break leaves cash fraud incidence unavailable after 2020. The primary inferential set is therefore

$$\mathscr{B} = \{(i,t) : i \in \mathscr{I},\ t = 2015,\dots,2020\}, \qquad |\mathscr{B}| = 24. \tag{2}$$

The 2021–2022 observations for checks and cards are retained for descriptive trends and out-of-year validation, but they are not used to create a falsely balanced extension. Figure 1 summarizes the full analytical sequence.

3.2 Measures and transformations

Payment share, S_{it}, is the percentage of total consumer payments by number made with instrument i. *Fraud incidence*, F_{it}, is the percentage of adopters reporting loss, theft, or fraudulent use during the preceding 12 months. It measures the share of users affected, not the financial value of fraud, the number of incidents, or uncompensated loss. *Security rank*, R_{it}, orders the assessed instruments from 1, the most secure, to 8, the least secure. A reverse-coded desirability measure is defined as

$$P_{it} = 9 - R_{it}, \tag{3}$$

so that larger values represent stronger perceived security.

Within-instrument variation is represented by

$$\Delta S_{it} = S_{it} - S_{i,t-1}, \qquad \Delta P_{it} = P_{it} - P_{i,t-1}, \tag{4}$$

while $F_{i,t-1}$ is used to preserve temporal ordering between prior adverse experience and current share change. For a cross-section in year t, standardization is

$$z_t(X_{it}) = \frac{X_{it} - \bar{X}_t}{s_{X,t}}, \tag{5}$$

where $\bar{X}_t$ and $s_{X,t}$ are the cross-instrument mean and population standard deviation.

3.3 Econometric specifications

The pooled model relates payment share to perceived security and fraud incidence while controlling for year effects:

$$S_{it} = \alpha + \beta_1 P_{it} + \beta_2 F_{it} + \lambda_t + \varepsilon_{it}. \tag{6}$$

Equation (6) describes cross-instrument structure but does not remove stable differences in acceptance, rewards, transaction records, liquidity, or cash-management needs.

The two-way fixed-effects specification adds instrument effects, μ_i:

$$S_{it} = \alpha + \beta_1 P_{it} + \beta_2 F_{it} + \mu_i + \lambda_t + \varepsilon_{it}. \tag{7}$$

Equivalently, define the double-demeaned variable

$$\ddot{X}_{it} = X_{it} - \bar{X}_{i\cdot} - \bar{X}_{\cdot t} + \bar{X}_{\cdot\cdot}. \tag{8}$$

The coefficients in Equation (7) are then identified from

$$\ddot{S}_{it} = \beta_1 \ddot{P}_{it} + \beta_2 \ddot{F}_{it} + \ddot{\varepsilon}_{it}, \tag{9}$$

which isolates within-instrument departures after common year movements are removed.

A stricter dynamic specification uses annual differences:

$$\Delta S_{it} = \alpha + \gamma_1 \Delta P_{it} + \gamma_2 F_{i,t-1} + \lambda_t + u_{it}. \tag{10}$$

All regression models use HC3 heteroskedasticity-consistent covariance estimates,

$$\widehat{\mathrm{Var}}_{\mathrm{HC3}}(\hat{\beta}) = (\mathbf{X}'\mathbf{X})^{-1}\mathbf{X}'\,\mathrm{diag}\left(\frac{\hat{e}_j^2}{(1-h_{jj})^2}\right)\mathbf{X}(\mathbf{X}'\mathbf{X})^{-1}, \tag{11}$$

where h_{jj} is the jth leverage value. Given the small aggregate panel, estimates are interpreted as structured associative evidence rather than causal effects.

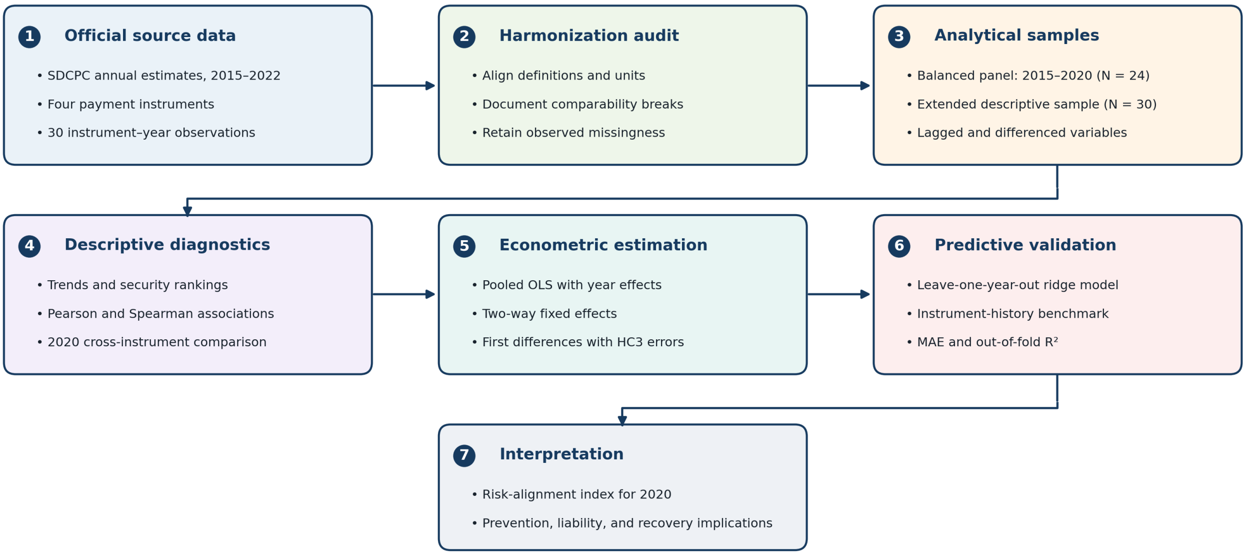


Figure 1. Analytical workflow from source-data harmonization to inference, out-of-year validation, and risk-alignment interpretation.

3.4 Predictive validation and alignment index

For each held-out year h, a ridge model is estimated on all observations with $t \neq h$. Let $\mathbf{z}_{it}$ contain standardized P_{it} and F_{it} plus one-hot instrument indicators. The training-fold estimator is

$$(\hat{\theta}_0^{(-h)}, \hat{\theta}^{(-h)}) = \arg\min_{\theta_0,\theta} \sum_{t\neq h} \left(S_{it} - \theta_0 - \mathbf{z}_{it}'\theta\right)^2 + 3\|\theta\|_2^2. \tag{12}$$

The comparison rule predicts a held-out observation with the corresponding instrument's mean share across the remaining years. With N out-of-fold predictions, performance is measured by

$$\mathrm{MAE} = \frac{1}{N}\sum_{j=1}^{N} |S_j - \hat{S}_j|, \tag{13}$$

$$R^2_{\mathrm{OOF}} = 1 - \frac{\sum_{j=1}^{N}(S_j - \hat{S}_j)^2}{\sum_{j=1}^{N}(S_j - \bar{S})^2}. \tag{14}$$

For the latest complete common year, 2020, the descriptive risk-alignment and usage indices are

$$A_{i,2020} = z_{2020}(P_{i,2020}) - z_{2020}(F_{i,2020}), \tag{15}$$
$$U_{i,2020} = z_{2020}(S_{i,2020}). \tag{16}$$

$A_{i,2020}$ is not a welfare or causal index. It identifies instruments whose perceived security is high or low relative to reported incident exposure and contrasts that position with standardized usage.

4. RESULTS

4.1 Payment use and incident exposure

Figure 2 shows markedly different trajectories. Cash declined from 33.3% of payment count in 2015 to 18.6% in 2020. Credit-card share increased from 18.3% in 2015 to 26.9% in 2020 and continued to 31.3% in 2022. Debit cards remained near 29% in 2022, while checks declined to 3.8%. These patterns are consistent with continued substitution toward cards, but they do not by themselves reveal whether risk perceptions caused the shift.

Table 2. Instrument-level descriptive statistics.

Instrument	Mean share	Latest share	Mean fraud	Latest fraud
Cash	27.43	18.59[a]	6.36	3.77[a]
Check	5.54	3.81	0.60	0.35
Credit card	23.92	31.27	6.16	10.32
Debit card	28.53	29.16	5.56	7.49

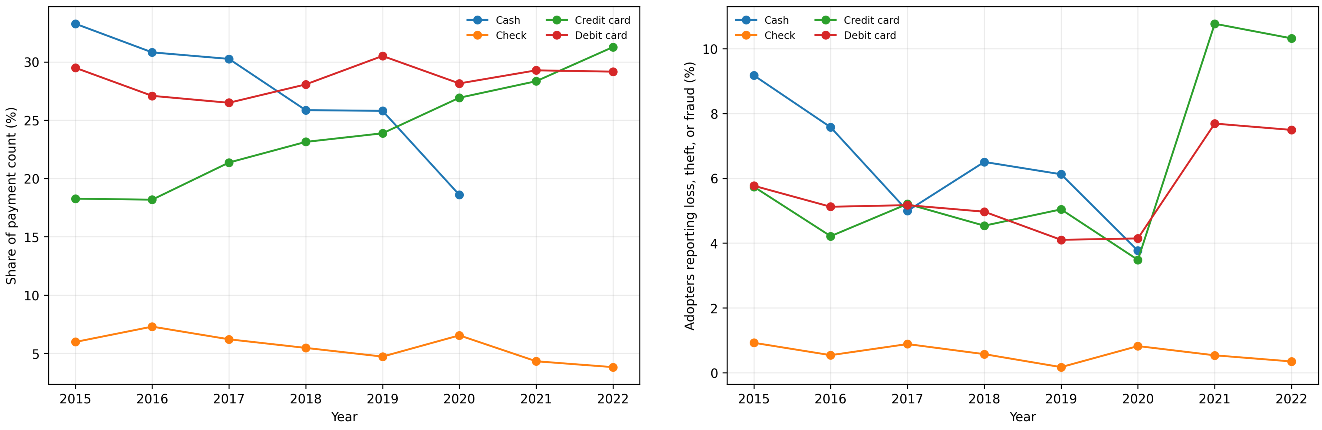
Shares and fraud incidence are percentages. Latest values refer to 2022 except [a]cash, which refers to 2020 because comparable later fraud observations are unavailable.

Fraud incidence did not move monotonically with use. Credit-card incidence was 3.5% in 2020, then rose above 10% in 2021 and remained 10.3% in 2022. Debit-card incidence reached 7.5% in 2022. Checks recorded far lower incidence, 0.35% in 2022, while their use continued to contract. The coexistence of high card use and elevated incident exposure is the empirical core of the fraud-protection paradox.

4.2 Perceived security and the protection paradox

The security rankings in Figure 3 reveal stable instrument ordering. Credit cards ranked first in perceived security in seven of eight years and second in the remaining year. Debit cards occupied the middle of the ranking, whereas cash was consistently near the bottom. In 2020, credit cards combined the strongest security score with a fraud incidence of 3.48%. Cash had a much weaker security score and a similar incident rate of 3.77%. Debit cards had greater incident exposure than both but also the largest payment share in that year.

The pooled correlation between fraud incidence and payment share is strongly positive (Pearson $r = .862$, $p < .001$; Spearman $\rho = .774$, $p < .001$). This should not be interpreted as a behavioral benefit of fraud. Instruments that are used frequently create more exposure opportunities and differ in acceptance, rewards, liquidity, and consumer protections. Perceived security has a weaker pooled association with payment share (Pearson $r = .220$, $p = .243$). The descriptive evidence



(a) Payment-count shares by instrument. **(b)** Adopters reporting loss, theft, or fraud.

Figure 2. Payment use and reported adverse experience. Cash fraud incidence is unavailable after 2020.

Table 3. Balanced-panel regression results, 2015–2020.

Variable	Pooled	Two-way FE	First diff.
Security score	0.353	$3.984^{\dagger}$	—
Standard error	(0.524)	(2.264)	
Fraud incidence	3.861^{***}	2.204	—
Standard error	(0.338)	(1.664)	
Security change	—	—	0.733
Standard error			(2.771)
Lagged fraud	—	—	−0.267
Standard error			(0.318)
Year effects	Yes	Yes	Yes
Instrument effects	No	Yes	Differenced
Observations	24	24	20
R^2	.833	.947	.148

HC3 standard errors in parentheses. Dependent variable is payment share in the first two models and annual percentage-point share change in the third. $^{\dagger}p < .10$; $^{***}p < .001$.

therefore suggests that perceived protection is not a direct inverse of reported event incidence.

4.3 Pooled and within-instrument estimates

Table 3 separates the pooled composition from within-instrument evidence. In Model 1, fraud incidence has a coefficient of 3.86 ($p < .001$), implying that instruments with higher fraud incidence also tend to have higher payment shares. Security desirability is not significant. The model explains 83.3% of variation, largely because the instruments occupy persistently different positions.

After instrument fixed effects are added in Model 2, the fraud coefficient falls to 2.20 and is not statistically significant ($p = .185$). The security coefficient becomes positive but remains imprecisely estimated (3.98, $p = .078$). Model 3 offers the stricter change-based test. Neither a change in security perception (0.73, $p = .791$) nor prior-year fraud incidence (−0.27, $p = .401$) is associated with the annual change in payment share. The contrast between Models 1 and 2–3 indicates that the positive pooled relationship is primarily a between-instrument pattern rather than evidence that rising fraud increases subsequent use.

4.4 Out-of-year validation

The leave-one-year-out model achieves an R^2 of .873, indicating that stable instrument identity and the two risk-related variables reproduce much of the cross-instrument structure. Its MAE is 2.90 percentage points. The simpler instrument-mean benchmark has a lower R^2 of .857 but a better MAE of 2.71. Figure 4 shows that the ridge predictions broadly track observed shares, yet their year-specific errors do not consistently improve on the baseline.

This result is substantively important. High predictive R^2 does not establish incremental explanatory value when instrument identity already captures persistent differences. Security perceptions and fraud incidence add insufficient short-run information to outperform a history-only rule on absolute error. A credible payment-risk model therefore needs more granular variables, including transaction frequency, merchant acceptance, rewards, disputed amounts, reimbursement, authentication friction, and recovery time.

4.5 Risk alignment and usage intensity

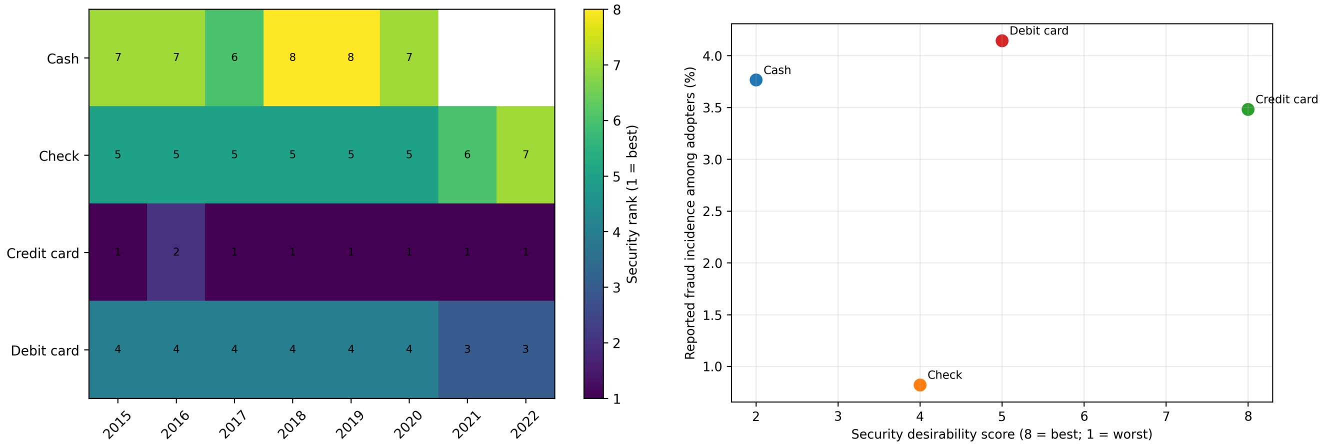
The 2020 alignment comparison in Figure 5 provides a compact view of the paradox. Credit cards combine positive protection alignment and above-average usage. Checks also have positive protection alignment because incident exposure is low, but usage is well below average. Debit cards display above-average usage despite negative risk alignment, while cash is below average on both protection alignment and usage.

These differences show why security cannot be evaluated through one dimension. Low fraud incidence does not guarantee continued relevance, and high usage does not demonstrate successful prevention. The absence of a significant relationship between lagged fraud and subsequent share change reinforces this point. Consumers may treat the payment instrument as a bundle of transaction utility and post-incident safeguards, not as a simple ranking of event probabilities.

5. DISCUSSION

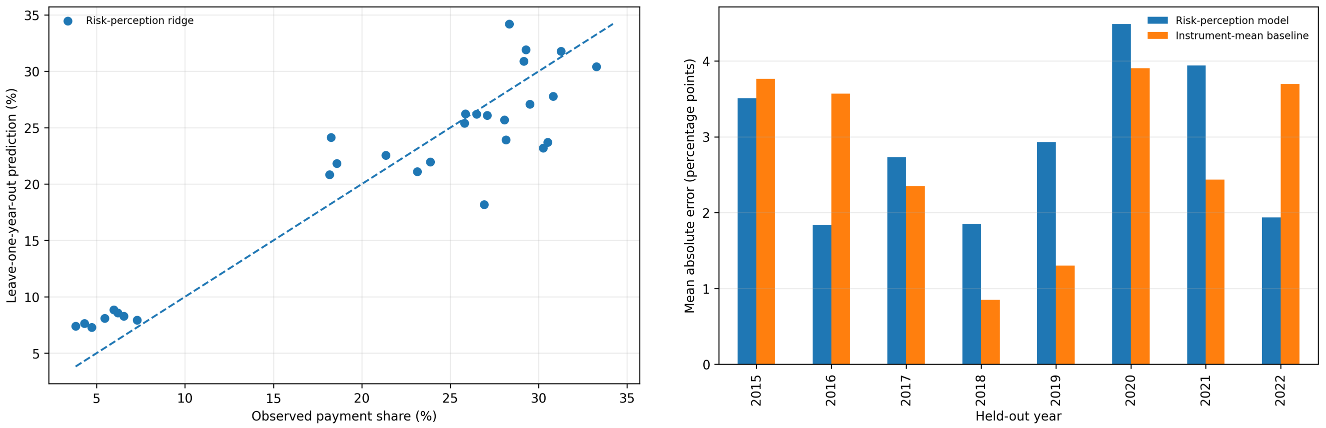
5.1 Interpreting the paradox

The central finding is not that consumers disregard security. It is that measured incident frequency and perceived protection capture different constructs. Credit-card users may encounter fraudulent use while still perceiving the instrument as secure because transactions are recorded, anomalies can be detected, credentials can be replaced, and disputed charges may be resolved. The source data do not directly measure



(**a**) Perceived-security rankings. (**b**) Security and incident exposure in 2020.

Figure 3. Perceived security and reported adverse experience.



(**a**) Observed and held-out predictions. (**b**) Absolute prediction error by year.

Figure 4. Out-of-year validation of the risk-perception model.

reimbursement or recovery quality, so this mechanism remains an interpretation rather than a tested mediation path. Nevertheless, it is consistent with the stable security ranking and continued growth of credit-card share despite elevated affected-user rates.

Exposure also matters. A widely accepted instrument used frequently across physical and digital channels creates more opportunities for incidents to be observed. Pooled comparisons therefore confound risk with transaction volume and instrument function. The collapse of the fraud coefficient after instrument controls is consistent with this exposure explanation. It also demonstrates why provider fraud statistics should be normalized by usage, value, channel, and active accounts before they are treated as consumer-protection indicators.

The pattern for checks provides the opposite case. Their low incident incidence does not preserve use because payment choice reflects convenience, acceptance, speed, and integration with digital commerce. This finding aligns with evidence that convenience and ecosystem conditions are central to electronic-payment substitution [1, 6]. Security is necessary, but it is not sufficient to sustain an instrument.

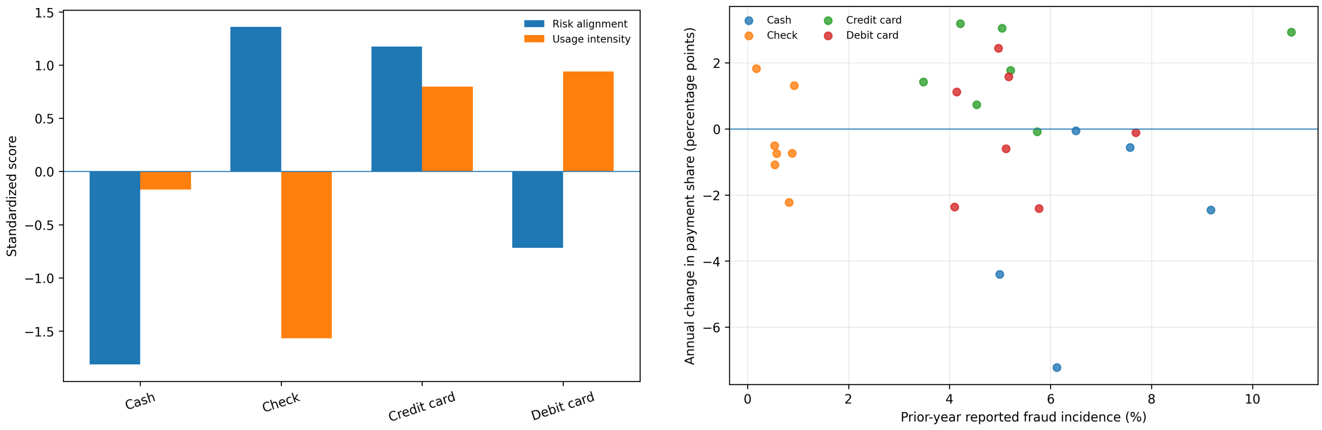
5.2 Implications for FinTech providers

Payment firms should distinguish four layers of protection: prevention, detection, containment, and recovery. Prevention includes authentication, tokenization, device controls, and transaction screening. Detection concerns timely notifications and anomaly recognition. Containment limits further loss after a credential is compromised. Recovery includes dispute access, provisional credit, transparent status information, and restoration of the account or instrument. A dashboard that reports only gross fraud events can understate improvement in recovery or overstate protection when users bear substantial unresolved harm.

Product design should also minimize the friction created by security controls. Excessive authentication, false declines, or opaque account holds can reduce utility even when they lower fraud. The appropriate objective is not minimum incident count at any cost, but minimum expected consumer harm subject to reliable access. This principle is particularly important as mobile interfaces and open-data services add participants to the transaction chain [14, 20].

5.3 Implications for regulators and researchers

Consumer-protection reporting would benefit from a consistent outcome set: affected-user rate, fraudulent value relative to legitimate value, unreimbursed loss, time to detection, time



(a) Risk alignment and usage intensity. **(b)** Lagged incidents and annual share change.

Figure 5. Descriptive alignment and within-instrument change.

to resolution, false-positive burden, repeat victimization, and complaint escalation. These measures should be reported by payment rail and initiation channel. Such disclosure would make it possible to distinguish an instrument that has frequent but rapidly resolved events from one that has fewer but severe and unrecoverable losses.

Future research should connect representative payment diaries with incident-level administrative records. Longitudinal linkage could test whether an adverse event changes the same consumer's subsequent payment mix and whether reimbursement moderates that response. Heterogeneity by income, age, digital capability, and access is also essential because adoption and protection are not distributed uniformly [2, 21, 18]. Finally, studies of payment innovation should evaluate whether new interfaces merely change initiation or genuinely alter the allocation of risk and responsibility within the financial system [17, 16].

6. LIMITATIONS

Individual longitudinal records are not used, but rather annual estimates of the aggregate. It cannot prove that someone who was victimized altered their payment habits and it cannot differentiate between incident probability and the number and the value of transactions. Incidence of fraud is self-reported by adopters and includes loss, theft and fraudulent use. Does not disclose if the user incurred an amount that wasn't covered by reimbursement. The security measure is a rank security that is related to the instruments in the survey.

Only 24 observations are on the balanced panel. The statistical power of fixed-effects and first-difference estimates are thus small, and not to be interpreted as definitive nulls. Cash series for 2021–2022 is not used for incident comparisons due to questionnaire comparability. The ridge model was not a forecasting system but a validation exercise and when compared to the instrument-mean baseline on MAE it does not perform better, which further emphasises the need for more detailed microdata. Lastly, the evidence is specific to U.S. consumers, and may not be immediately applicable to markets that have different liability rules, card acceptance, real-time payment systems, and cash reliance.

7. CONCLUSION

Consumer-payment security cannot be inferred from fraud incidence alone. From 2015 through 2022, credit cards combined the strongest perceived security, a rising payment share, and comparatively high reported incident exposure. The positive pooled association between fraud incidence and use disappears when the analysis focuses on changes within instruments. Security changes and lagged fraud likewise do not explain annual share changes in the balanced panel, and a risk-perception prediction model does not improve absolute error over an instrument-history benchmark.

The evidence supports a broader interpretation of protection. Consumers appear to value the expected consequence and recoverability of an incident alongside its probability, while convenience and acceptance continue to shape use. Financial-technology providers and regulators should therefore assess prevention, detection, containment, reimbursement, and resolution together. A payment system is not secure merely because few incidents are recorded; it is secure when users face low expected harm and can recover promptly when controls fail.

REFERENCES

[1] M. Brown, N. Hentschel, H. Mettler, and H. Stix, "The convenience of electronic payments and consumer cash demand," *Journal of Monetary Economics*, vol. 130, pp. 86–102, 2022.

[2] O. Shy, "Low-income consumers and payment choice," *Research in Economics*, vol. 74, no. 4, pp. 292–300, 2020.

[3] J. Boden, E. Maier, and R. Wilken, "The effect of credit card versus mobile payment on convenience and consumers' willingness to pay," *Journal of Retailing and Consumer Services*, vol. 52, p. 101910, 2020.

[4] S. Talwar, A. Dhir, A. Khalil, G. Mohan, and A. K. M. N. Islam, "Point of adoption and beyond: Initial trust and mobile-payment continuation intention," *Journal of Retailing and Consumer Services*, vol. 55, p. 102086, 2020.

[5] X.-M. Loh, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and Y. K. Dwivedi, "Switching from cash to mobile payment: What's the hold-up?" *Internet Research*, vol. 31, no. 1, pp. 376–399, 2021.

[6] S. Moghavvemi, X. M. Tan, S. W. Phoong, and S. Y. Phoong, "Drivers and barriers of mobile payment adoption: Malaysian merchants' perspective," *Journal of Retailing and Consumer Services*, vol. 59, p. 102364, 2021.

[7] Y. Liu, J. Luo, and L. Zhang, "The effects of mobile payment on consumer behavior," *Journal of Consumer Behaviour*, vol. 20, no. 3, pp. 512–520, 2021.

[8] S. Y. Ahn and Y. Nam, "Does mobile payment use lead to overspending? the moderating role of financial knowledge," *Computers in Human Behavior*, vol. 134, p. 107319, 2022.

[9] G. Migliore, R. Wagner, F. S. Cechella, and F. Liébana-Cabanillas, "Antecedents to the adoption of mobile payment in china and italy: An integration of utaut2 and innovation resistance theory," *Information Systems Frontiers*, vol. 24, no. 6, pp. 2099–2122, 2022.

[10] A. A. Bailey, C. M. Bonifield, A. Arias, and J. Villegas, "Mobile payment adoption in latin america," *Journal of Services Marketing*, vol. 36, no. 8, pp. 1058–1075, 2022.

[11] N. Upadhyay, S. Upadhyay, S. S. Abed, and Y. K. Dwivedi, "Consumer adoption of mobile payment services during covid-19: Extending meta-utaut with perceived severity and self-efficacy," *International Journal of Bank Marketing*, vol. 40, no. 5, pp. 960–991, 2022.

[12] K. Song, P. Wu, and S. Zou, "The adoption and use of mobile payment: Determinants and relationship with bank access," *China Economic Review*, vol. 77, p. 101907, 2023.

[13] A. M. Sahi, H. Khalid, A. F. Abbas, and S. F. A. Khatib, "The evolving research of customer adoption of digital payment: Learning from content and statistical analysis of the literature," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 7, no. 4, p. 230, 2021.

[14] R. Chan, I. Troshani, S. Rao Hill, and A. Hoffmann, "Towards an understanding of consumers' FinTech adoption: The case of Open Banking," *International Journal of Bank Marketing*, vol. 40, no. 4, pp. 886–917, 2022.

[15] A. Boot, P. Hoffmann, L. Laeven, and L. Ratnovski, "Fintech: What's old, what's new?" *Journal of Financial Stability*, vol. 53, p. 100836, 2021.

[16] D. Broby, "Financial technology and the future of banking," *Financial Innovation*, vol. 7, p. 47, 2021.

[17] V. Ferrari, "The platformisation of digital payments: The fabrication of consumer interest in the eu fintech agenda," *Computer Law & Security Review*, vol. 45, p. 105687, 2022.

[18] T. Yang and X. Zhang, "Fintech adoption and financial inclusion: Evidence from household consumption in china," *Journal of Banking & Finance*, vol. 145, p. 106668, 2022.

[19] M. Cheng and Y. Qu, "Does bank FinTech reduce credit risk? Evidence from China," *Pacific-Basin Finance Journal*, vol. 63, p. 101398, 2020.

[20] Z. He, J. Huang, and J. Zhou, "Open banking: Credit market competition when borrowers own the data," *Journal of Financial Economics*, vol. 147, no. 2, pp. 449–474, 2023.

[21] M. Jünger and M. Mietzner, "Banking goes digital: The adoption of fintech services by german households," *Finance Research Letters*, vol. 34, p. 101260, 2020.

[22] K. Foster, C. Greene, and J. Stavins, "2022 survey and diary of consumer payment choice," Federal Reserve Bank of Atlanta, Research Data Report 2023-03, 2023.