Enhancing Payment Security in U.S. Restaurants: The Case for Wireless Tableside Terminals

Hailey Rockandel
Fall 2024

Summary

Society versus U.S. Restaurants. Issue is payment security.

In most U.S. restaurants, it is standard practice for servers to take a patron's credit card out of sight to a fixed payment terminal to process the transaction after a meal. From both a security and customer convenience standpoint, reducing the visibility of a patron's credit card is inefficient, as it increases the risk of fraud and takes longer for servers to close tables due to the back-and-forth action. Instances of credit card fraud in restaurants across the country, year after year, highlight the urgent need for the industry to modernize its payment practices and adopt handheld wireless solutions.

Studies:

1. A study might involve writing a computer program to scrape the Consumer Financial Protection Bureau (CFPB) for recorded entries of consumer fraud in restaurants to demonstrate the prevalence and patterns of fraudulent activities in the industry.
2. A study might involve field research where a student dines at ten restaurants in the Boston area, five using fixed point-of-sale (POS) terminals and five using wireless POS terminals. The student will document how long their credit card is taken out of sight while the transaction is being processed, as well as the total time it takes to close the bill at each restaurant.
3. (Related) The student might interview the restaurant owners or managers at each of the ten establishments, exploring their preferences for different POS systems and gathering insights on any experiences with fraud.

Introduction

The U.S. restaurant industry lags behind its international counterparts in adopting advanced payment technologies [1]. Reliance on outdated or insecure payment systems exposes establishments to fraud and data breaches, undermining customers' trust and financial security [2]. For example, earlier this year, a restaurant employee in Louisburg was accused of inflating tip amounts and copying card information to use in other stores [3]. In Annapolis, a former waiter pleaded guilty to stealing customers' credit card information as part of a conspiracy scheme to commit access device fraud, swiping cards through a skimmer to steal

credit and debit card information [4]. In Fort Lauderdale, a waitress was found swiping diners' credit cards into her own device, making thousands of dollars' worth of unauthorized charges behind the scenes [5]. A West Knoxville waiter, employed at several restaurants in the region, served himself extra tips using stolen credit card information from his customers [6]. These instances of fraud are not solely attributed to lower-end establishments. In Manhattan, a high-end restaurant became the target of a sophisticated credit card skimming operation when a trusted staff member installed a skimming device on the restaurant's fixed point-of-sale (POS) terminal, collecting hundreds of credit card numbers from wealthy customers and selling the information on the dark web [7]. This technology-society clash resonates beyond local American patrons. On a popular online travel thread, a user from the U.K. expressed concern over the payment practices she encountered in New York, writing, "I'm worried and confused that in U.S. restaurants it seems common for staff to take credit cards away from you to process payment at tills. One has just been returned to me with a payment receipt with an added 8% tax and 20% tip, which I certainly had no chance to authorize or decline. In [the] U.K., you do not allow credit cards out of your grasp or sight to avoid risk of card cloning or overcharging" [8]. The vulnerability of fixed POS terminals in restaurants and credit card fraud in the U.S. remains a complex issue. While fixed terminals are the standard payment technology nationwide, they are subject to distinct security challenges and operational constraints compared to more advanced and modern wireless systems. Are instances of fraud in restaurants related to the type of terminal used? This technology-study plan proceeds under the null hypothesis that using fixed POS terminals in U.S. restaurants never leads to instances of credit card fraud or reduced operational efficiency compared to wireless tableside terminals.

Background

Payment Practices in the U.S.

Research cites two main reasons American restaurants have yet to adopt tableside payment practices: tipping culture and chip-and-signature credit cards [9]. The U.S. is known as one of the "tip-happiest" countries in the world [10]. As an American custom, tipping is expected when dining at a restaurant, with patrons leaving a gratuity to show appreciation for the service provided. In other parts of the world, like many regions in Europe, a service charge is already included in the bill, alleviating the need for the patron to calculate an added gratuity [9]. Prior research suggests that adopting tableside payment practices in the U.S. would make for an uncomfortable and awkward interaction between patrons and servers, as servers would linger while patrons calculate their tips [11]. However, looking north to our neighbors in Canada, tipping culture is equally as prevalent, yet restaurants have successfully adopted wireless tableside payment practices [12].

When the U.S. officially adopted EMV (Europay, Mastercard, and Visa) technology in 2015, most card issuers implemented a chip-and-signature system as opposed to chip-and-PIN.

EMV payment technology, which is exponentially more secure than magnetic stripe (magstripe) cards, transmits payment data to the card reader during a transaction by generating a unique code for every purchase (Figure 1). Pressures from the federal government in 2015 forced merchants into a rushed deadline for installing new equipment to comply with EMV cards. While the transition ushered in a major improvement in digital payment controls, "the U.S. implemented EMV in the most insecure way" [13] by operating with a hybrid chip-and-signature system rather than fully transitioning to chip-and-PIN. Chip-and-PIN cards are considerably more secure, requiring cardholders to create a PIN and enter that number at the point of sale to authenticate the transaction [14]. Meanwhile, chip-and-signature cards rely on a signature for each transaction to verify the cardholder's identity. Many standard handheld terminals are not set up for signatures and, as a result, may not be conducive to the standard chip-and-signature credit card in the U.S. [9].

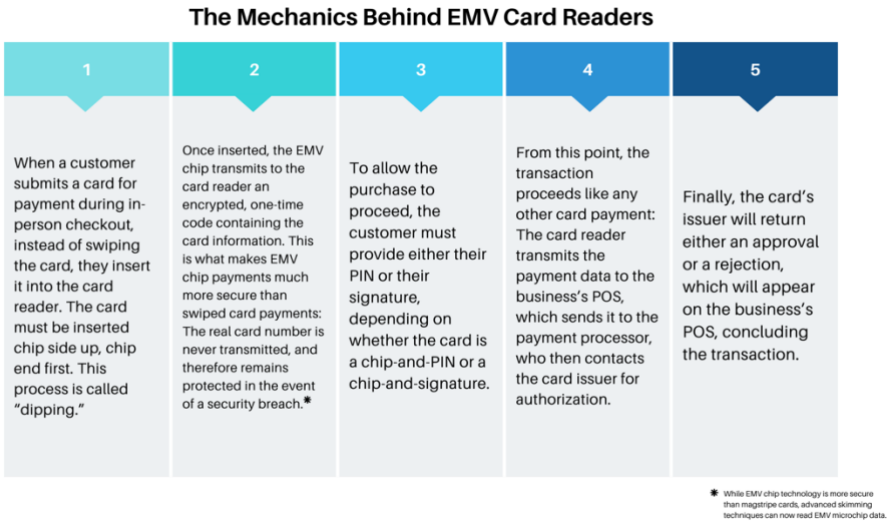


Figure 1. The Five Key Steps Involved in EMV Card Transactions [14]

Point-of-Sale Terminals

Globally, the Restaurant POS Terminal Market was estimated at USD $20.4 billion in 2023 and is projected to reach USD $30.4 billion by 2030 [15]. This market presents substantial growth opportunities "driven by several factors reflecting technological adoption, customer expectations, and industry needs" [15]. In 2024, 73% of Americans reported using credit or debit cards rather than cash when dining at restaurants [16]. With most patrons opting for card payments, restaurants must ensure their payment systems securely meet evolving consumer preferences.

Restaurants have two primary options for processing payments: fixed terminals or wireless tableside terminals. In 2023, the fixed terminal segment accounted for over 65% of the market share in the U.S. [17]. As the standard practice in U.S. restaurants, fixed terminals are stationary devices typically located near a server station in the back of an establishment, allowing staff to manage all transactions centrally. In terms of workflow, fixed terminals

involve the customer flagging the server to indicate they are ready for the bill, the server collecting the customer's payment method, bringing the card to the terminal to process the transaction, and finally, the server returning with the receipt for the customer to review, add gratuity, and sign. In comparison, wireless terminals process transactions through a single handheld device at the table [2]. Rather than taking the customer's card out of sight, tableside terminals allow the server to process the payment directly at the table, enabling the customer to review the transaction, add gratuity, and complete the process without delay. Wireless POS terminals can increase turnover, on average, by eight minutes a table, allowing a restaurant to serve significantly more diners, thereby positively impacting the bottom line [9], [13]. From a security standpoint, "the more links involved in the process, the greater the potential for fraud" [13]. Not only does efficiency drive revenue, but it also enhances the overall customer experience by reducing wait times and improving the convenience of the payment process.

Liability, Security Vulnerabilities, and Skimming

In restaurants, the burden of liability for fraud depends on how the transaction is processed. For card-present fraud, where the customer physically swipes, inserts, or taps their card, the merchant is liable if their payment terminals are not EMV chip card compliant. The introduction of EMV technology in 2015 forced businesses to upgrade their systems; otherwise, failure to do so meant assuming responsibility for counterfeit fraud and related costs. For card-not-present fraud, where the customer does not physically present the card, liability shifts to the credit card issuer [18].

Whether restaurants use stationary or wireless terminals, every establishment must comply with PCI DSS: The Payment Card Industry Data Security Standard. Grouped into six control objectives, these standards include the following: build and maintain a secure network and systems, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy [19]. In lay terms, PCI compliance ensures that restaurants protect their customer's sensitive payment information by establishing secure systems and practices to reduce the risk of data breaches [20].

Restaurants present an ideal environment to commit credit card fraud as a customer's card is out of sight for several minutes when closing the cheque. Conventional fraud practices have been carried out through credit card skimming. Criminals can add skimming devices to payment terminals, appearing as plastic overlay shells that look identical to the top of a POS terminal. POS skimming devices can steal card data, allowing the perpetrator to re-encode said data onto counterfeit cards, which can then be used for unauthorized transactions [21]. The introduction of EMV technology was designed to make it incredibly challenging for fraudsters to conduct skimming, given that chip cards generate a unique token for each transaction [22]. However, when there is a will, there is a way. To get around EMV microchips,

fraudsters have turned to an advanced form of skimming: shimming. Shimming, best described as “skimming 2.0”, uses a thin reader called a ‘shim’ that fits into a card terminal slot and can read EMV microchip data in the same manner that skimmers can read magstripe data, collecting the details required to authenticate and process future transactions [22], [23]. Contrary to the common belief that card skimming is a practice of the past, credit card skimming attacks surged by 700% in 2022 due to the rise of shimming techniques [23]. Given the covert nature of credit card shimming, there are limited ways for customers to proactively protect themselves from such fraud; the number one being contactless payment methods [23]. In the context of the restaurant industry, contactless payments like Apple Pay and Google Pay are only feasible if payment terminals are brought to the customer’s table via a wireless device. With the rise of advanced shimming techniques, the need to transform payment practices in American restaurants has never been more urgent. The following proposed studies will reveal the prevalence, patterns, and impacts of credit card fraud in U.S. restaurants while also exploring the effectiveness of fixed versus wireless payment terminals in mitigating such risks.

Materials and Methods

1. Scrape the Consumer Financial Protection Bureau (CFPB) Consumer Complaint Database for Restaurant Fraud

The CFPB publishes a Consumer Complaint Database that updates daily and is freely available to the public (Figure 2) [24]. Within the Consumer Complaint Database, complaints can be filtered by various variables. For this study, complaints will be filtered to the state of Massachusetts and by the search term “restaurant” (Figure 3). Matches that fit this filter (44) will be scraped using an open-source web-crawling framework like BeautifulSoup or Scrapy. NumPy will be used to clean and analyze the data. Finally, statistical software like Tableau or Excel will be used to support data visualization. This study requires proficiency in programming, web scraping, data cleaning, statistical analysis, and data visualization.

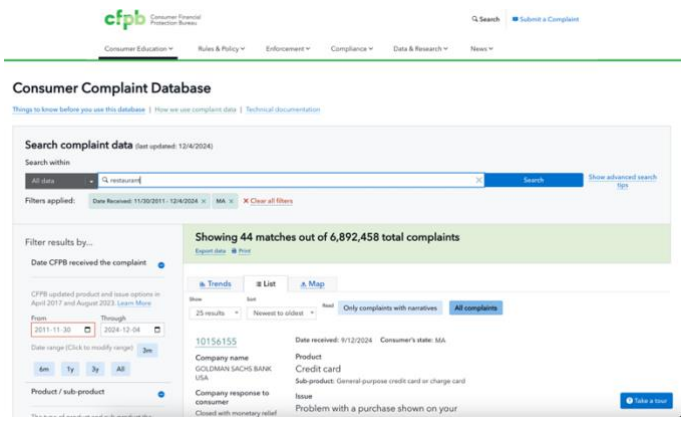


Figure 2. The Consumer Financial Protection Bureau’s Consumer Complaint Database

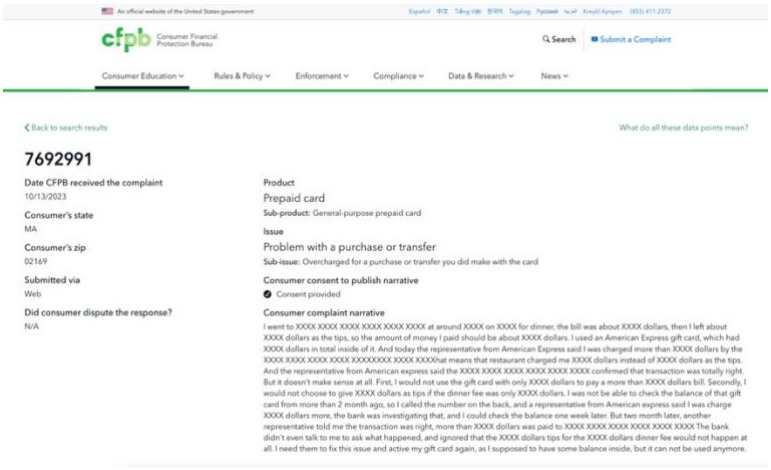


Figure 3. Example of a Complaint Entry

2. Field Research on POS Terminals

This study requires access to restaurants in the Boston area that are willing to participate, specifically ten establishments divided equally between those using fixed and wireless POS terminals. Resources required include a stopwatch or smartphone with a timer application and a note-taking application for recording observations. Key skills include effective communication for engaging with restaurant staff, attention to detail for accurate timing and documentation, data organization abilities, and basic data analysis skills to summarize findings.

3. Interviews with Restaurant Owners and Managers

Necessary resources include contact information for the restaurant owners and managers, audio recording equipment or a note-taking device for capturing interview responses, consent forms to adhere to ethical research practices, and a structured interview guide with key questions. This study requires strong interpersonal and interviewing skills, knowledge of ethical research protocols such as obtaining informed consent, and the ability to synthesize qualitative findings.

Studies

Desired Outcome

The envisioned result is for U.S. restaurants to shift business practices by adopting wireless tableside terminals to reduce the number of links involved in the payment process, thereby lowering the risk of credit card fraud. As a design statement, the goal is to:

Construct wireless handheld terminals
Such that U.S. restaurants adopt tableside payment practices.

Two primary studies can be done to examine the prevalence of credit card fraud in U.S. restaurants and compare payment processes between fixed and wireless POS terminals, complemented by a third related study to gather qualitative insights from industry stakeholders.

Study 1. Scrape the CFPB Consumer Complaint Database for Restaurant Fraud

A study might write a computer program to scrape the CFPB Consumer Complaint Database for recorded entries of consumer fraud tied to restaurants. To keep the dataset manageable, entries will be filtered to the state of Massachusetts (Figure 2). Data analysis will focus on categorizing the type of fraud (unauthorized charges, skimming, delayed processing) to identify specific vulnerabilities, granted that information is provided in the entry. The complaints will also be categorized by the submission date to analyze temporal trends.

Study 2. Field Research on POS Terminals

A study might involve dining at ten restaurants in the Boston area, five of which use fixed terminals, and five that use wireless terminals to process payments. To minimize variability in the results, selected restaurants will be matched for similar characteristics such as cuisine type, customer volume, prices, and neighborhood demographics. This controlled selection approach will help ensure consistency across the sample. Participants will order comparable meal combinations at each restaurant to reduce potential confounding factors related to meal type or price, further standardizing the research conditions. At all ten restaurants, the student will document the total time it takes to close the bill, from the initial request for the cheque to the final payment confirmation, capturing the entire transaction process. In the subset of five restaurants with fixed payment terminals, the student will document the total time the credit card is away from the table, tracking the server's payment processing workflow.

Study 3. (Related) Interviews with Restaurant Owners and Managers

To complement the second study, interviews may be conducted with the owners of the ten restaurants visited to gather qualitative insights into the operational and decision-making factors shaping payment processing practices. The interviews will explore the rationale behind their choice of POS systems, their awareness of fraud risks, and the effectiveness of their current fraud prevention strategies. This study aims to examine the systemic and business-level factors that influence payment security and efficiency, offering context and depth to the quantitative findings from the other studies.

Predicted Events

Suppose Study 1 was conducted and revealed an upward trend in consumer complaints submitted to the Consumer Financial Protection Bureau (CFPB) related to credit card fraud in restaurants. Such a study would raise the question of how to enhance payment security measures in restaurants to mitigate the risk of credit card fraud.

Suppose Study 2 was conducted and revealed that wireless tableside terminals positively impact transaction efficiency and customer security compared to fixed terminals. Such a study would raise the question of how restaurants in the U.S. can adopt wireless POS terminals as a standard business practice.

The decision-makers most likely to respond to such studies are journalists, restaurant managers and owners, restaurant customers, the CFPB, and the Payment Card Industry Security Standards Council (PCI SSC) (See Appendix B). Journalists want to publish stories that garner engagement, which would likely detail stories of fraud to draw public attention. Meanwhile, restaurant managers and owners want positive coverage of their restaurants, so their establishments continue getting business and do not face public scrutiny.

A likely response by restaurant managers and owners about the studies to journalists would be to capitalize on positive customer reviews and leverage external endorsements that can help build a positive company image to mitigate controversial news coverage.

Media attention could further motivate customers who have been directly impacted by weak payment security practices in restaurants to mobilize. These customers might voice their concerns publicly by writing to the PCI SSC, calling out poor practices on social media, or seeking compensation from restaurants or credit card issuers.

If media attention escalates and U.S. citizens amplify their complaints, the CFPB could take a series of responsive actions. The agency might launch an investigation into the patterns of credit card fraud in restaurants, analyzing complaint data to identify systemic vulnerabilities. Based on its findings, the CFPB could recommend best practices to restaurants, including adopting wireless POS systems, improving staff training, and enhancing compliance with PCI Data Security Standards.

Additionally, the CFPB might collaborate with the PCI SSC to address identified vulnerabilities and advocate for updated security standards tailored to restaurant payment systems. In cases where significant negligence or violations are found, the CFPB may take enforcement action, issuing fines or penalties against non-compliant establishments or payment processors.

Discussion

In summary, a study (Study 1) could reveal that credit card fraud in restaurants is on the rise, thereby countering the common belief that EMV-chip technology is a guaranteed safeguard from fraud. Another study (Study 2) could demonstrate that using wireless POS terminals increases operational efficiency, allowing restaurants to serve significantly more diners, thereby positively impacting the bottom line. The related study (Study 3) could offer qualitative insights into the perspectives of restaurant managers and owners on different POS systems and the operational challenges they encounter in implementing various payment solutions. Collectively, these studies could catalyze an industry-wide shift to wireless tableside terminals.

As with any scientific study, there is a possibility that the null hypothesis may not be rejected, and the results do not materialize as expected. If this is the case, and no correlation is found between increased credit card fraud and fixed POS terminals, then none of the predicted events will occur. However, this technology-study plan would still provide valuable insights by reassuring the public that there is no immediate cause for concern regarding secure payment practices in U.S. restaurants. In this case, the proposed related study (Study 3) would be of limited value, as further investigation into restaurant owners' preferences for payment systems and experiences with fraud would be less relevant. Even if no direct correlation is found between credit card fraud and fixed POS terminals, the studies could spark ongoing conversations about the state of payment security in the American restaurant industry. After all, the U.S. is one of the few Western countries where servers regularly take customers' credit cards out of sight to process payments. Ultimately, even in the absence of a direct correlation, these studies could enhance consumer trust and provide a clearer picture of payment security practices.

References

[1] J. Lamb, “How Restaurants Can Improve Credit Card Security with Handheld Devices,” Forbes. December 21, 2023. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2023/12/21/how-restaurants-can-improve-credit-card-security-with-handheld-devices/

[2] K. Omar, “Pay at the Table Best Practices: A Complete Guide for Restaurants,” Lightspeed. June 19, 2023. [Online]. Available: https://www.lightspeedhq.com/blog/pay-at-the-table/

[3] H. Schmidt, “Former Louisburg restaurant employee accused of tip inflation, credit card theft,” KCTV. August 20, 2024. [Online]. Available: https://www.kctv5.com/2024/08/20/former-louisburg-restaurant-employee-accused-tip-inflation-credit-card-theft/

[4] United States Attorney’s Office, “Former Waiter Pleads Guilty in Credit Card Fraud Scheme,” District of Maryland. November 10, 2015. [Online]. Available: https://www.justice.gov/usao-md/pr/former-waiter-pleads-guilty-credit-card-fraud-scheme

[5] WPLG Local 10, “Police: Fort Lauderdale waitress charged thousands to diners’ credit cards,” YouTube. January 5, 2024. [Online]. Available: https://www.youtube.com/watch?v=4C7cnrj7ti0

[6] D. Jacobs, “West Knoxville water pilfered credit card data from employee of U.S. Attorney’s office,” Knoxville News. August 16, 2017. [Online]. Available: https://www.knoxnews.com/story/news/2017/08/16/west-knoxville-waiter-sentenced-credit-card-identity-thefts/572513001/

[7] D. Bartoszek. “Restaurant Frauds (Scam Examples & Prevention),” Upmenu. August 23, 2024. [Online]. Available: https://www.upmenu.com/blog/restaurant-fraud/

[8] Lucycocozoe. “Credit card payments out of sight?” Tripadvisor. May 23, 2023. [Online]. Available: https://www.tripadvisor.com/ShowTopic-g60763-i5-k14402703-o10-Credit_card_payments_out_of_sight-New_York_City_New_York.html

[9] E. Cannon, “Why Swiping Your Card at the Table Lags in the US,” NerdWallet. January 29, 2018. [Online]. Available: https://www.nerdwallet.com/article/credit-cards/pay-at-table-dining-credit-cards

[10] V. Postrel, “Tipping Culture is out of control. Trump and Harris would make it worse,” The Seattle Times. August 30, 2024. [Online]. Available: https://www.seattletimes.com/opinion/tipping-culture-is-out-of-control-trump-and-harris-

would-make-it-worse/#:~:text=Americans%20have%20long%20been%20among,whose%20research%20focuses%20on%20tipping

[11] C. Nnamani, “Restaurant Tableside Payments: What You Need to Create A Better Customer Experience,” The Bottom Line. August 1, 2023. [Online]. Available: https://squareup.com/us/en/the-bottom-line/operating-your-business/tableside-payment-experience

[12] D. Faraldo, “Why do Canadians Love Pay-At-Table Payment Options,” Divvia. [Online]. Available: https://divvia.ca/why-do-canadians-love-pay-at-table-payment-options/

[13] Nachreiner, “How the US Continues to Lag Behind in Secure Electronic Payments,” Forbes. December 7, 2020. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2020/12/07/how-the-us-continues-to-lag-behind-in-secure-electronic-payments/

[14] Stripe, “What are EMV chip cards? How EMV works and why it’s so secure,” February 2, 2023. [Online]. Available: https://stripe.com/resources/more/what-are-emv-chip-cards

[15] Globe News Wire, “Restaurant Point of Sale Report 2024 – Growth of Mobile Point-of-Sale (mPOS) Systems Drives Adoption of Mobile-compatible Restaurant Management Software – A US$30.4 Billion Market by 2030,” Research and Markets. November 21, 2024. [Online]. Available: https://www.globenewswire.com/news-release/2024/11/21/2984942/28124/en/Restaurant-Point-of-Sale-Terminal-Report-2024-Growth-of-Mobile-Point-of-Sale-mPOS-Systems-Drives-Adoption-of-Mobile-compatible-Restaurant-Management-Software-A-US-30-4-Billion-Mark.html

[16] D. Krook, “The Ultimate Guide to Payment Processing for Restaurants,” TouchBistro. [Online]. Available: https://www.touchbistro.com/blog/the-ultimate-guide-to-payment-processing-for-restaurants/

[17] Global Market Insights, “Restaurant Point of Sale (POS) Terminal Market Size,” June 2024. [Online]. Available: https://www.gminsights.com/industry-analysis/restaurant-pos-terminals-market

[18] Toast, “Everything You Need to Know about Restaurant Fraud Prevention,” [Online]. Available: https://pos.toasttab.com/blog/restaurant-fraud?srsltid=AfmBOop4ThqaKfvmE_J_5wZNs98sn25ApoetiCLR-inh9IR4AcZJt_ME

[19] S. Baykara, “Control Objectives,” PCI DSS Guide. January 1, 2022. [Online]. Available: https://pcidssguide.com/pci-dss-control-objectives/#google_vignette

[20] Kickfin, “What is Restaurant PCI Compliance,” [Online]. Available: https://kickfin.com/blog/restaurant-pci-compliance/

[21] United States Secret Service, “ATM & POS Skimming,” [Online]. Available: https://www.secretservice.gov/investigations/skimming

[22] P. Thangavelu, “Can chip cards be skimmed,” Bankrate. November 25, 2024. [Online]. Available: https://www.bankrate.com/credit-cards/advice/chip-cards-skimming-shimming/#shimmed

[23] Chargebacks, “Credit Card Shimmers,” February 13, 2023. [Online]. Available: https://chargebacks911.com/credit-card-shimmers/

[24] Consumer Financial Protection Bureau, “Consumer Complaint Database,” [Online]. Available: https://www.consumerfinance.gov/data-research/consumer-complaints/search/?date_received_max=2024-12-05&date_received_min=2011-11-30&page=1&searchField=all&size=25&sort=created_date_desc&tab=List

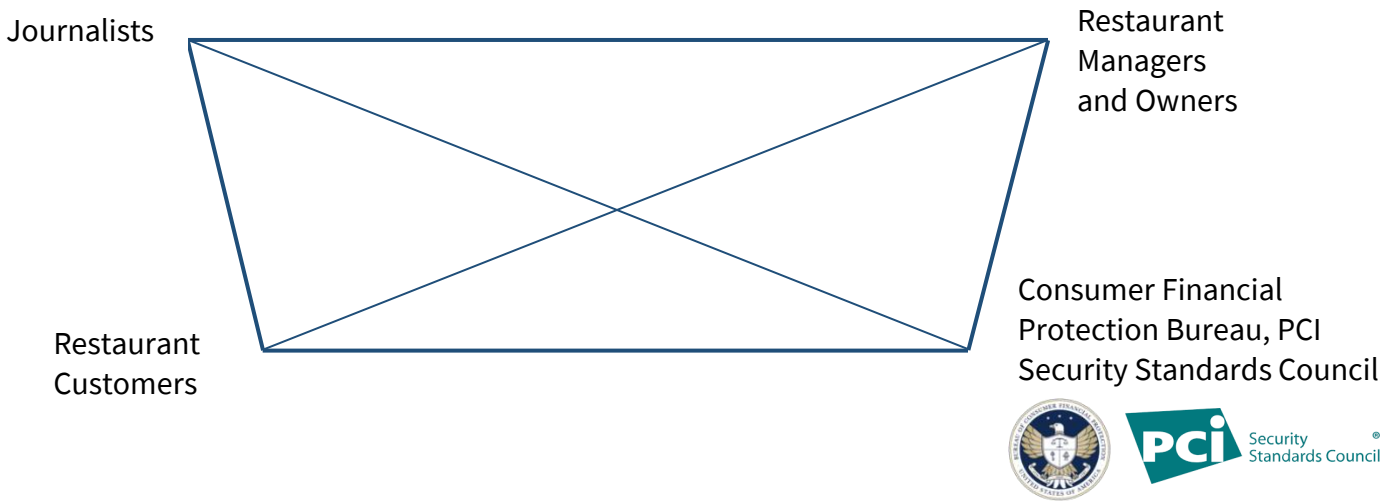
APPENDIX A

Key Conflict in this Study

	American Society	U.S. Restaurants
Both Want	Secure payment systems in restaurants	
Requirements	provided the payment process is fast and transparent	provided the system minimizes disruption to existing workflows
	A study in this project would aid society in reducing vulnerabilities related to payment fraud. Issue: payment security.	

APPENDIX B

Decision-Makers Projected Response to the Proposed Study



(A) Journalists versus Restaurant Managers and Owners

	Journalists	**Restaurant Managers and Owners**
Both Want	Restaurants in the news	
Requirements	provided stories draw attention and engagement	Provided stories portray positive coverage of the restaurants
Direct Actions in Response to Study	publish stories that highlight controversies in the restaurant industry around payment practices and fraud	Adjust operations, address criticisms
Indirect Actions to counter direct actions	offer follow-up coverage documenting improvements	leverage positive customer reviews and external endorsements to build a positive image

(B) Consumer Financial Protection Bureau versus Restaurant Managers and Owners

	Consumer Financial Protection Bureau	**Restaurant Managers and Owners**
Both Want	Protection of customers' financial information	
Requirements	Investigate and address systemic vulnerabilities that enable credit card fraud	Implement secure payment systems and adhere to regulations to avoid penalties

Direct Actions in Response to Study	Release studies and guidelines focused on mitigating credit card fraud in restaurants	Update payment infrastructure (e.g., EMV-compliant terminals)
Indirect Actions to counter direct actions	Partner with industry groups to disseminate best practices about fraud prevention	Enhance staff training on fraud prevention

(C) Payment Card Industry (PCI) Security Standards Council versus Restaurant Managers and Owners

	PCI Security Standards Council	**Restaurant Managers and Owners**
Both Want	Protection of cardholder data and reduced instances of fraud	
Requirements	Enforce compliance with PCI DSS (Data Security Standards)	Understand and implement PCI DSS to maintain compliance and avoid penalties
Direct Actions in Response to Study	Conduct audits to ensure compliance	Upgrade payment systems, ensure proper data encryption, train staff on secure payment practices
Indirect Actions to counter direct actions	Offer guidance, training resources, and tools to help restaurants meet compliance	Collaborate with payment processors and vendors to simplify compliance, advocate for more practical standards for smaller establishments

APPENDIX C

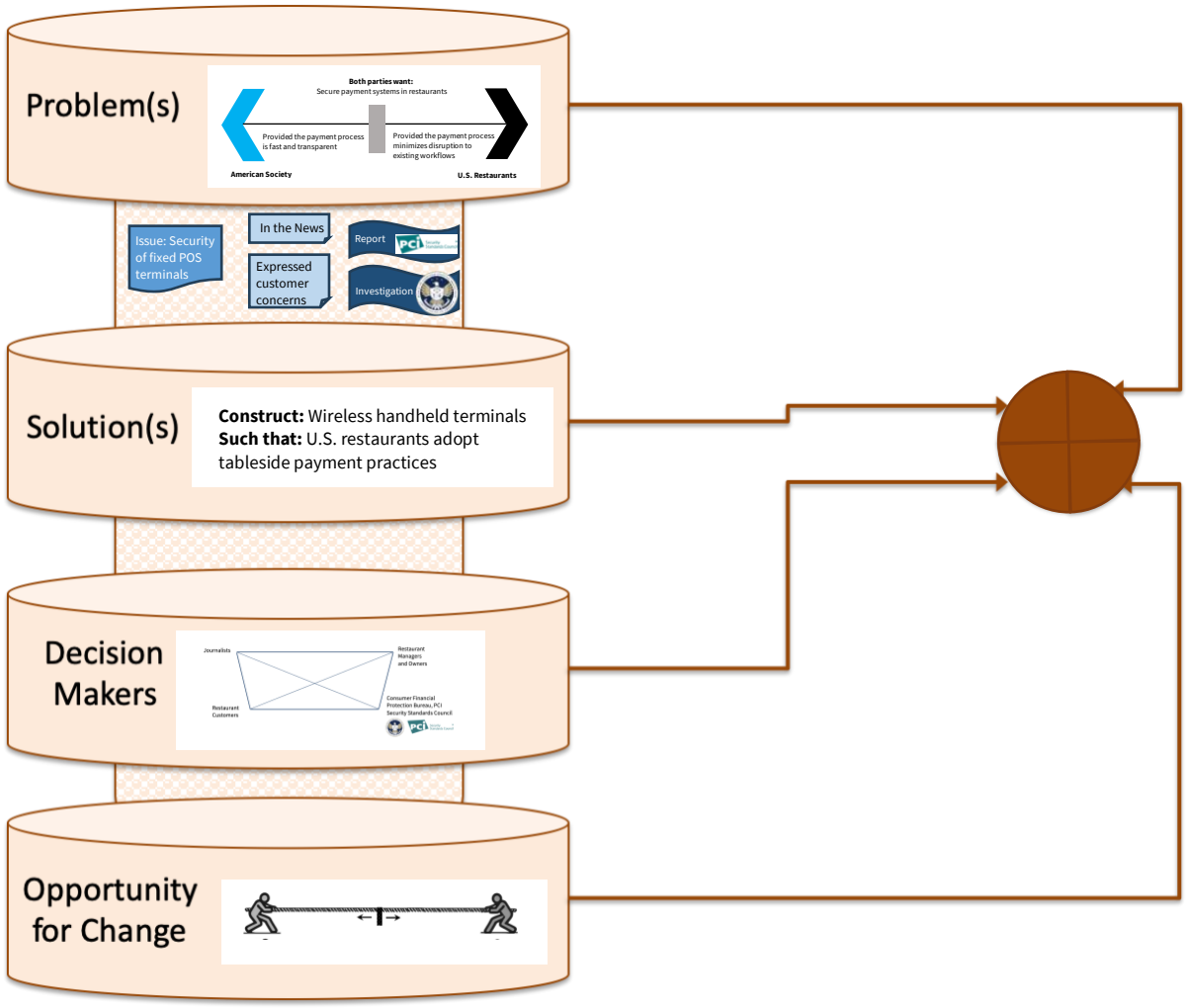
Projected Response Timeline

Projected responses are below. Time flows downwards.

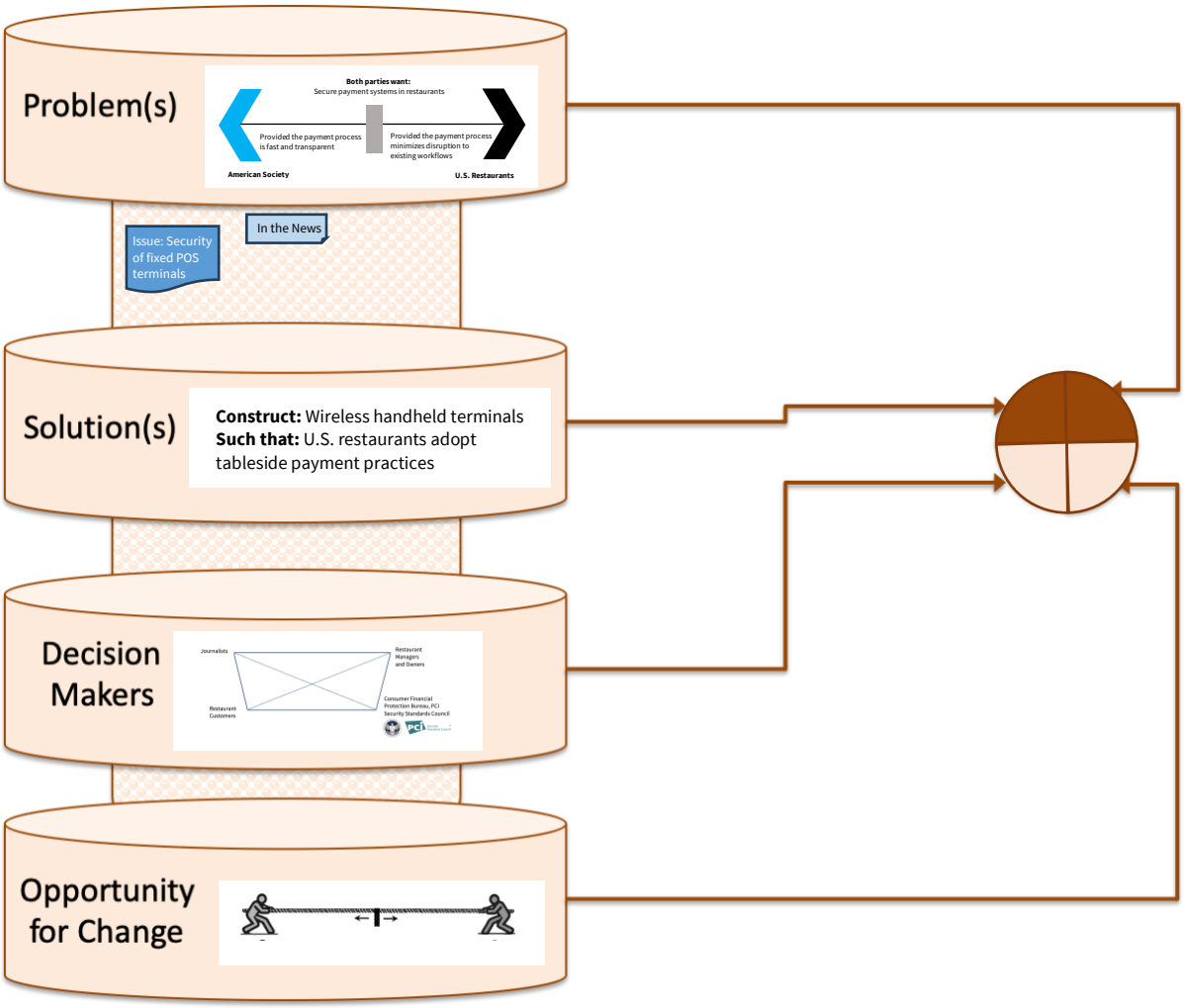
Study	Journalists	Restaurant Customers	Consumer Financial Protection Bureau	Restaurant Managers and Owners
The issue is payment security in U.S. restaurants.				
	News stories about credit card fraud in restaurants.			Respond by adopting secure technology solutions, like tableside payment systems, to enhance security and restore customer trust.
		Expressed concern, seek compensation for fraud.		
			Investigation.	
				Construct wireless handheld terminals **such that** U.S. restaurants adopt tableside payment practices.

APPENDIX D

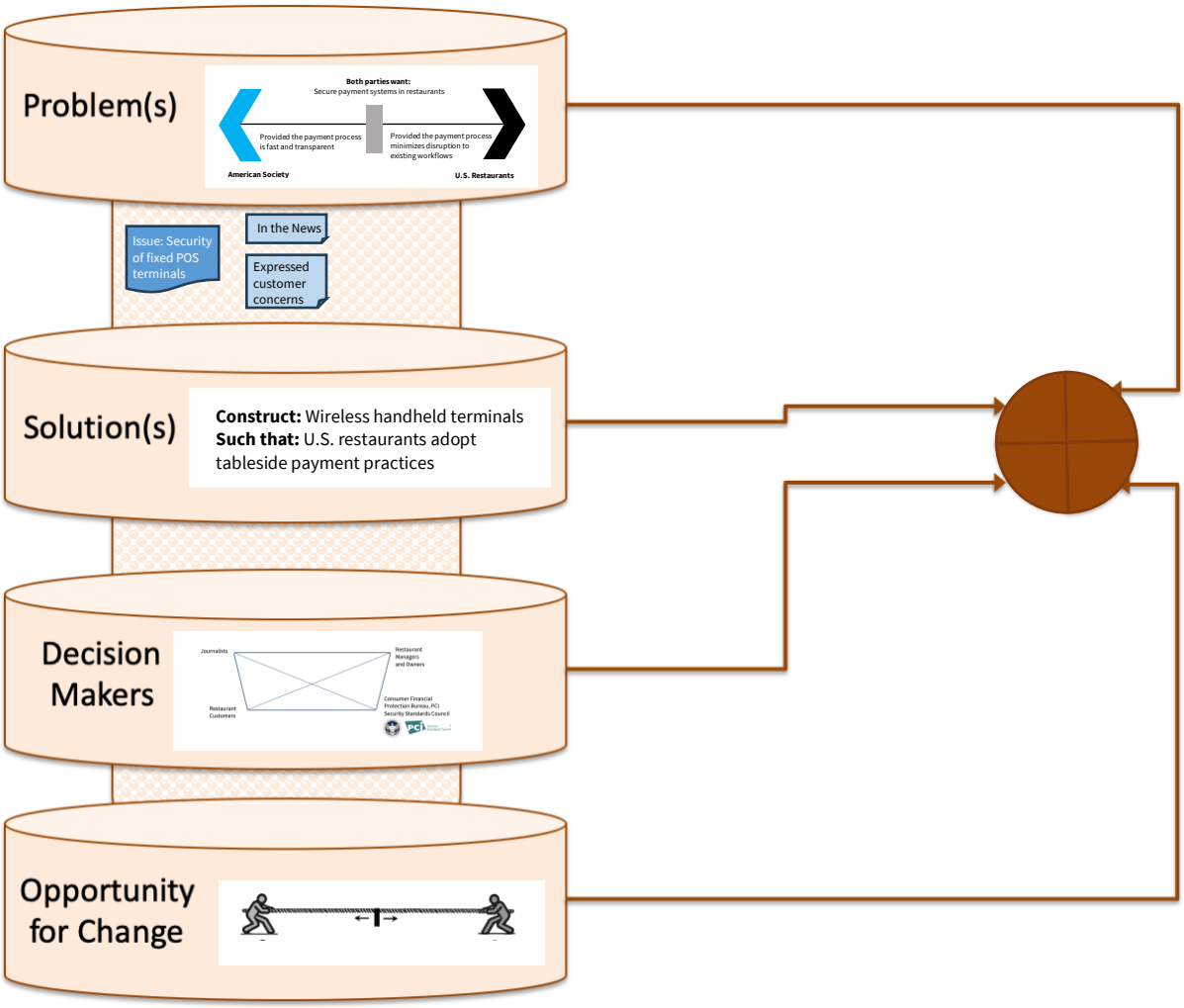
Help the Helpers Model Opportunity for Change



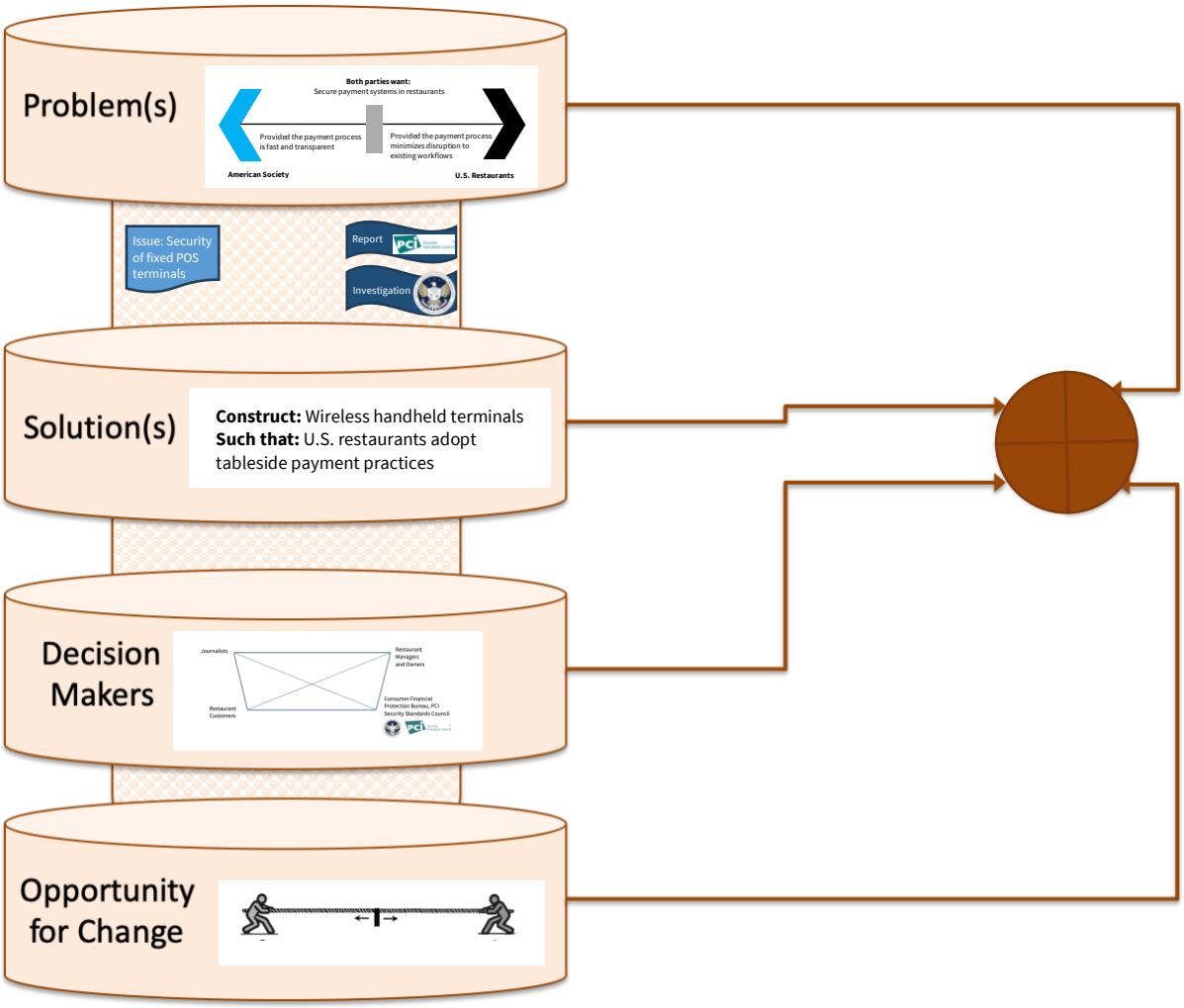
(a) Predicted events all occur, foretells change



(b) Media response alone, foretells no change



(c) No CFPB investigation, but strong concerns expressed by customers, foretells change



(d) CFPB investigation and PCI SSC reports, foretells change