Privacy and Security Evaluation of Mobile Payment Applications Through User-Generated Reviews

URVASHI KISHNANI*, NAHEEM NOAH*, SANCHARI DAS, and RINKU DEWRI, Ritchie School of Engineering and Computer Science, University of Denver

Mobile payment applications are crucial to ensure seamless day-to-day digital transactions. However, users' perceived privacy- and security-related concerns are continually rising. Users express such thoughts, complaints, and suggestions through app reviews. To this aim, we collected 1, 886, 352 reviews from the top 50 mobile payment applications. Furthermore, we conducted a mixed-methods in-depth evaluation of the privacy- and security-related reviews resulting in a total of 163, 210 reviews. Finally, we implemented sentiment analysis and did a mixed-methods analysis of the resulting 52, 749 negative reviews. Such large-scale evaluation through user reviews informs developers about the user perception of digital threats and app behaviors. Our analysis highlights that users share concerns about sharing sensitive information with the application, confidentiality of their data, and permissions requested by the apps. Users have shown significant concerns regarding the usability of these applications (48.47%), getting locked out of their accounts (38.73%), and being unable to perform successful digital transactions (31.52%). We conclude by providing actionable recommendations to address such user concerns to aid the development of secure and privacy-preserving mobile payment applications.

CCS Concepts: • **Security and privacy → Web application security**; **Mobile platform security**; **Usability in security and privacy**.

Additional Key Words and Phrases: e-payment security, mobile applications, review analysis, privacy.

ACM Reference Format:
Urvashi Kishnani, Naheem Noah, Sanchari Das, and Rinku Dewri. 2022. Privacy and Security Evaluation of Mobile Payment Applications Through User-Generated Reviews. 1, 1 (September 2022), 24 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

With the immense use of smartphones and the widespread growth of cashless payments, mobile payment applications are becoming central to performing transactions on a day-to-day basis. Dahlberg et al. define mobile payment as "payments for goods, services, and bills with a mobile device (such as a mobile phone, smartphone, or personal digital assistant (PDA)) by taking advantage of wireless and other communication technologies" [12]. Currently, there are several mobile payment applications available in mobile app stores to download and perform digital transactions. The number of such e-payment applications is also increasing at a rapid rate [34] and are used for peer-to-peer transactions, making in-store cashless purchases, and enabling quick payments across borders. About US$ 8.56 trillion worth of digital payments are projected to be made in the year 2022 alone, and this figure is expected to grow at an annual growth rate of 12.77%, which will result in a projected total amount of US$ 13.85 trillion by the year 2026 [56].

*Both authors contributed equally to this paper.

Authors' address: Urvashi Kishnani; Naheem Noah; Sanchari Das; Rinku Dewri, {firstname.lastname}@du.edu, Ritchie School of Engineering and Computer Science, University of Denver.

With the rising popularity of digital payments, it is essential to note that the data on mobile payment applications can be susceptible to cyberattacks such as man-in-the-middle attacks, replay attacks, impersonation, and unauthorized access [3]. This is because these mobile payment applications often access sensitive data, such as Personally Identifiable Information (PII) [17, 22, 51, 52] including name, address, and banking information comprised of debit and credit card details. It is predicted that the total cost of cybercrime across the globe will be about US$ 10.5 trillion by 2025, with the main attack surface being about 200 zettabytes of data [11].

As we note the privacy and security risks associated with these mobile payment applications, it is also critical to understand the user perspectives [13, 14, 46]. One of the ways we can get real-time feedback on the applications is through the reviews submitted by users of these applications, as studied earlier by Das et al. and Noman et al. [15, 47]. A wealth of information about these applications can be obtained through the reviews left by the users on the online app stores, such as the reviews submitted in the Google Play Store [41, 49]. These reviews form an essential crowdsourced resource of feedback that can be beneficial to both the application developers and other users [9, 32, 33, 59]. Negative reviews can be used to assess where an application may be lacking. These reviews are one of the leading outlets of concerns and frustrations that these users express regarding their experience with the application [59]. The major issues for an application are often highlighted in these reviews, where a pattern emerges through repeated complaints by different users on the same features of the applications.

In this study, we collected 1, 886, 352 reviews from the Google Play Store of the top 50 mobile payment applications. We then performed a text-based analysis on the reviews to extract and analyze those reviews that pertaining to users' privacy and security concerns related to the apps, mainly focusing on the negative reviews (52, 749). We performed a manual analysis of a subset of these reviews (1, 410 reviews) to provide a detailed overview of the reviews collected from a qualitative perspective. Through this study, we make the following contributions from our work:

- To the best of our knowledge, this is the first in-depth analysis of mobile payment applications through review-based analysis. To this, we collected the reviews of the top 50 mobile payment applications (based on the application download counts) to understand their level of performance from a user perspective.
- We analyzed these reviews to understand the extent of users' concerns about privacy and security while using mobile payment applications. This is critical as these reviews are expected to be predominantly from real users of the applications. After that, we followed a detailed mixed-methods approach which provided an in-depth analysis from the quantitative and the qualitative sides.
- We identified the thematic distribution of these concerns in the reviews. Such categorization and analysis of the reviews via human and automated coding helped us understand the user concerns about these applications' privacy, security, and usability. Based on our analysis and prior work in this research area (described in detail in section 2), we give actionable recommendations in section 6 which will be beneficial for the developers of these applications.

2 RELATED WORK

To lay the foundation of our work, we investigated the existing literature and academic work in three parts: prior research on mobile applications, prior work on the privacy and security of mobile payment applications, and finally prior work on analyzing reviews.

2.1 Privacy and Security of Mobile Apps

There is a wealth of research about the privacy and security of all mobile applications, irrespective of their connection with digital payments. Researchers have developed open-source tools to help understand mobile applications' security and privacy status. For example, Mobile Security Framework (MobSF) [1] is a widely used open-source tool used for security and malware analysis of mobile applications, RiskInDroid [42] is used for risk analysis specifically for Android applications, and AndroBugs [37] is used for vulnerability assessment of Android apps. However, most of these tools are used in research or industry and are not readily used or understood by the common users of mobile apps. To enable users to make informed decisions, there is an effort to build recommendation systems for users to understand the security and privacy aspects of the applications, such as that created by Zhu et al. [68]; however, their adoption has been slow due to privacy concerns [50].

Concepts of privacy, security, and network usage are a black box to most smartphone users, who do not understand how mobile applications work. Such users are often concerned with the requests for permissions that applications require [19]. Vidas et al. mention that not all permissions requested by the applications are used [61], which increases the attack surface and leaves the users susceptible to data leaks. Wei et al. uncover that the number of permissions on Android platforms tends to increase; specifically, those permissions deemed dangerous [63]. Ferreira et al. summarize that the top permissions that users are not comfortable sharing are contact information, profile data, and access to messages and calls [20]. Users are often unaware of the data that is collected by the applications and express both discomfort and surprise once they are made aware [4]. When it comes to mobile payment applications, the sensitivity of data and the concerns of users increase as these applications often require users' PII and banking information.

2.2 Privacy and Security of Payment Apps

Mobile payment methods are an integral and increasing part of a user's purchases, both online and on-site [7]. With the growing use, convenience, integration of these applications with the current telecommunication and financial structures, and compatibility with devices, these apps are soon becoming unavoidable. With the plethora of available options for mobile payment apps and the rapid integration of these apps in everyday use, mobile users are bound to adopt and use these applications. These mobile payment applications face particular barriers to widespread adoption. Fife and Orjuela have found that users are more concerned about privacy and security of personal information when using mobile applications compared to performing similar tasks on a computer [21].

Through their research, Huang and Liu show that the users' privacy concerns affect the perceived risk and trust of the mobile payment application, but this does not significantly impact the intention for usage [27]. Thus, usage of mobile payment applications is continued, despite these privacy concerns, as users are inclined to use these mobile payment services for convenience and needs [53]. However, Johnson et al. point out that adoption of these mobile payment systems has been slow, notwithstanding the associated advantages [30]. Further, they reveal that factors such as ease of use and perceived security by the users influence an individual's intentions for using these services.

Mobile payment applications heavily rely on sensitive and personal information disclosed by users, such as PII and banking details. Various factors influence the willingness of users to disclose such information. Yang et al. conducted two qualitative surveys that show that self-disclosure is formed by how users perceive the benefits of disclosing such information, whether the user perceives the privacy settings and privacy policies to be effective, and how the user perceives the risk of information disclosure [66]. Similarly, Gong et al. find that privacy assurance approaches can decrease users' concerns about self-disclosure in mobile payment applications [24]. Based on these findings, we evaluate

users' perception of mobile applications via reviews as one of the main channels for users to express their concerns is through reviews.

2.3 User Reviews of Mobile Apps

Mobile app reviews are often viewed as crowdsourced opinions of an app which indicate both the quality of and sentiments towards the application [9, 32, 33, 59]. Khalid et al. show how mobile reviews fit into the crowdsourcing framework and uncover some of the crowdsourcing activities performed by the users via these reviews [33]. They identify that users contribute by requesting new features, sharing recommendations for other users, stating problems and reporting (informally) bugs, and giving out suggestions for developers. In their paper, McIlroy et al. discuss that app reviews are rich in information that reflects a user's experience of the application [41]. However, this data is often unstructured, informal, and noisy. They propose a way to automate the process of labeling issues raised by users in their reviews. However, their analysis is limited to that of only 20 applications across ranging domains.

Vasa et al. show how the rating given by the user correlates to the length of the review. In particular, they find that users that leave negative and critical reviews of applications (i.e., those accompanied with 1 or 2-star ratings) often write longer reviews [59]. Our research similarly focuses on negative reviews related to privacy and security. Cen et al. create a model for providing a risk assessment of mobile applications based on user comments by labeling comments [9]. However, aside from the labels, their model does not classify the comments into broader categories. Vu et al. developed a keyword-based framework for classifying user reviews into different categories and concerns [49]. Our work focuses on the reviews from mobile payment applications and categorizes these reviews as is relevant for the e-payment domain.

3 METHOD

For our research, we collected the reviews of the top 50 mobile payment applications from the Google Play Store. We performed text-based analysis to filter the privacy and security-related reviews and applied sentiment analysis to collect the negative reviews focused on user privacy and security concerns. Furthermore, we performed an in-depth thematic analysis of a subset of these reviews through manual coding and automated analysis. In the following subsections, we describe our data collection, keyword extraction, data preprocessing, sentiment analysis, and thematic analysis processes. The overview of the method is provided in Figure 1.

As mentioned in the introduction, we defined mobile payments as "payments for goods, services, and bills with a mobile device (such as a mobile phone, smartphone, or personal digital assistant (PDA)) by taking advantage of wireless and other communication technologies" [12]. Additionally, we defined mobile payment applications as applications that are used to access electronic payment services for various activities using mobile wallets [5, 40]. Here we included any applications intended for digital transactions irrespective of the business model being B2B or B2C.

3.1 Data Collection

In Google Play Store, we selected the "Finance" category and the "Mobile payment" subcategory to determine the mobile payment applications for which we wanted to collect reviews. Then, from the applications enlisted, we selected the applications that met the criteria of at least $1M$ downloads. We also expanded our search by searching on Google Play Store with the keyword "mobile payment", which provided more results. Finally, we compiled the two lists, removed duplicates, and selected the top 50 mobile payment applications based on the download counts.

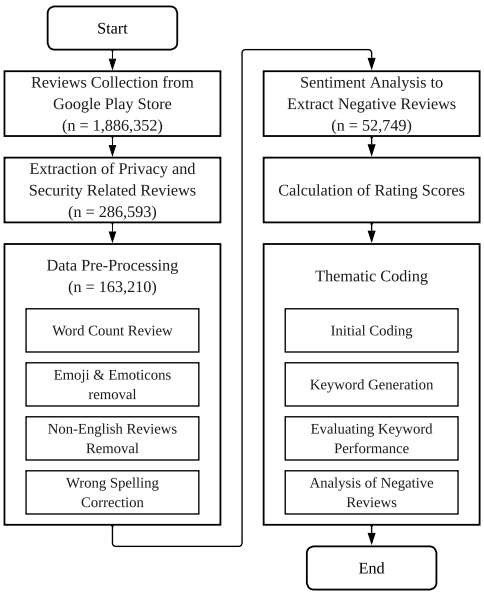

Fig. 1. Overview of the Study Design in a Flowchart

Table 1. User App Reviews Themes Definitions, Review Distribution Across Different Categories, Precision (P), Recall (R), and F1 Scores of the Reviews, and Top Three Keywords Of Individual Themes

Theme	**Theme Definition**	**No. of Negative Reviews**	**P(%)**	**R(%)**	**F1(%)**	**Top 3 Keywords**
Account Access	Reviews concerning users being prevented from legitimate access to their accounts	20431 (38.73%)	90.14	92.75	91.43	access, password, login
Usability	Reviews concerning usability or interface issues of the mobile payment applications	25566 (48.47)	94.07	83.45	88.44	update, install, installed
Transaction	Reviews concerning inhibitions for a successful financial transaction	16624 (31.52%)	88.40	77.22	82.43	transaction, transfer, wallet
User Info	Reviews about the usage of information requested by the mobile payment applications to verify the identity of the account	6609 (12.53%)	96.30	74.29	83.88	verify, debit card, identity
Confidentiality	Reviews concerning exposure of users' PII or sharing of data to the third-parties or other users	651 (1.23%)	87.50	87.50	87.50	private, privacy, public
Permission	Reviews concerning permissions for the mobile payment applications that are requested from the user	717 (13.60%)	80.00	100.00	88.89	permission, location, GPS

After that, we used the google-play-scraper [1] library to collect the reviews of the selected 50 applications. We capped the review collection to 100, 000 reviews per application. Our app review collection was done in May 2022. In total, we collected 1, 886, 352 user reviews associated with 50 mobile payment applications.

3.2 Privacy and Security Reviews Extraction

From all the collected reviews, our study primarily focuses on those related to privacy and security. To determine the set of privacy and security keywords to extract these reviews, we leveraged previously existing works that have also extracted privacy and security content from a wide range of data repositories [28, 36]. This helped us determine our primary set of keywords. However, we realized these primary keywords do not essentially cover the review extraction. For instance, terms like "account", "transaction", "credit", "debit", "card" etc. may or may not be attributed to privacy and security reviews based on their usage or occurrence. We introduced a secondary keyword list and an addendum list to solve this. Essentially, reviews with at least one secondary keyword and an addendum keyword would be tagged as privacy- or security-related review. An example would be "account lock" which has the addendum keyword "lock" or "transaction block" which has the addendum keyword "block". The full list of primary, secondary, and addendum keywords is available in Table A1. This improved the quality of the extracted privacy and security reviews. The keyword selection was made through five rounds of discussion between the researchers. The reviews extraction was done by a Python script that filters the reviews based on the collected keywords. Upon completion of the extraction, we were left with 286, 593 privacy- and security-related reviews.

3.3 Data Preprocessing

Data preprocessing plays a major role in cleaning the reviews and making them available for further analysis. For this phase, we performed the following tasks:

3.3.1 Word Count Review. We are specifically interested in detailed and unambiguous reviews, so we created a baseline of at least 100 characters in a review. This is related to the work done by [47] where they analyzed the user reviews of Facebook collected from blog posts. We believe that privacy and security issues require special attention from the reviewer and hence should be detailed. Therefore, based on Noman et al.'s work [47], we have filtered and removed the reviews that have less than 100 characters.

3.3.2 Emoji and Emoticon Removal. Emotional expressions are conveyed using emojis and emoticons. While emoticon serves as facial expression formulated from keyboard characters and punctuation, emojis are actual images used to express emotions. Therefore, emojis and emoticons complicate data analysis if not adequately handled. While an option would be to convert the emoji into words that pronounce their meaning, available dictionaries that perform the conversion into textual content still struggle to do so efficiently [57]. Therefore, we chose to remove these emojis and emoticons. This was done by creating a Python script that identifies them based on their Unicode characters and removes them from the review.

3.3.3 Non-English Reviews Removal. Mobile payment applications are used globally, so reviews appear in different languages. Our study focused on English-based reviews considering that our data modeling would be specific to English-written reviews. However, it is essential to note that some reviews have a mixture of English and other languages; we

[1] https://pypi.org/project/google-play-scraper/

leveraged the Python library langdetect [2] to determine the language of a review. Based on langdetect and our analysis strategy, we only analyzed the reviews which were tagged to be written in English.

3.3.4 Wrong Spelling Correction. Users are usually in a hurry to give reviews, which are mostly inputted from their mobile devices. Unfortunately, the sense of urgency and the structure of keyboard display in mobile devices increase the tendency of users to make typographic errors when giving reviews [49]. To ensure that incorrectly spelled words are corrected, we use the Python library language-tool-python [3]. Upon completing the data preprocessing, we were left with 163, 210 privacy- and security-related reviews.

3.4 Sentiment Analysis

Sentiment analysis is a Natural Language Processing (NLP) technique that helps extract subjective information in data to determine its positivity, negativity, or neutrality [31]. The sentiment analysis aimed to collect the negative privacy and security reviews from the resulting 163, 210 user reviews. To do this, we utilized the Textblob library [4], a lexicon-based sentiment analyzer which returns a polarity score within the range $[-1.0, 1.0]$. We determined positive reviews as reviews with polarity greater than 0, negative reviews with polarity less than 0, and neutral reviews with polarity equal to 0. As a result, we obtained 52, 749 negative privacy- and security-related reviews after this step.

3.5 Calculation of the Rating Scores

Along with leaving a review, users also leave scores for the applications. This score is denoted by a 0 to the 5-star rating assigned to the apps on Google Play Store [60]. This rating provides insights into the apps and informs the current state of an app. We calculated two rating scores for each application to facilitate a ranking of these applications. The first of these is the Privacy and Security Rating Score (PSR), which is calculated for all the privacy and security reviews of the application (i.e., on a total of 163, 210 reviews across all applications), and the second score is the Privacy and Security Negative Rating Score (PSNR), which is calculated for only the negative privacy and security reviews of the application (i.e., on a total of 52, 749 reviews across all applications). PSR and PSNR give the ratio of actually received scores to the total possible scores. The formulas for PSR and PSNR are given below:

$$PSR = \frac{\sum R}{5 \times NR}$$

$$PSNR = \frac{\sum NR}{5 \times NNR}$$

Where;

$\sum R$ = Sum of Reviews; this is the sum of all the scores of the privacy- and security-related reviews of the application

NR = Number of Reviews; this is the number of privacy- and security-related reviews of the application

$\sum NR$ = Sum of Negative Reviews; this is the sum of all the scores of the negative privacy- and security-related reviews of the application

NNR = Number of Negative Reviews; this is the number of negative privacy- and security-related reviews of the application

PSR = Privacy and Security Rating Score

[2] https://pypi.org/project/langdetect/
[3] https://pypi.org/project/language-tool-python/
[4] https://textblob.readthedocs.io/en/dev/

PSNR = Privacy and Security Negative Rating Score

3.6 Thematic Coding of Negative Privacy and Security Reviews

3.6.1 Initial coding. Thematic coding introduces qualitative analysis that enables common grouping of reviews into similar categories. Two independent coders randomly selected 100 reviews through open coding from the negative reviews and classified them into different thematic groupings using a Grounded Theory approach [18]. Six categories were identified: confidentiality, user information, permission, account access, transaction, and usability. Table 1 shows the definition of each identified term and the top three keywords for each category.

3.6.2 Keyword Generation. To further collect reviews that align with the six themes, we performed a text-based analysis to generate specific keywords that can be attributed to each theme. The two coders independently performed selective manual coding of 1,410 negative privacy and security reviews to achieve this. With inter-rater reliability of 86.1%, the coders proceeded to split the data into training and test dataset. 78% (n = 1088) served as training dataset while 22% (n = 322) served as testing data set. The coders manually generated keywords for each theme by going through all the reviews in the training dataset. Table 1 shows the top 3 keywords generated for each theme. The full list of keywords for each theme is available in Table A2. The keywords generated were applied to the test data to examine the performance of the keywords in correctly tagging the test reviews.

3.6.3 Evaluating Keyword Performance. The metrics used to evaluate the performance of the keywords are Precision, Recall, and F1 value. The Precision score determines the proportion of identifications that were correct, Recall determines the proportion of actual positives that were identified correctly, while the F1 score conveys the balance between the precision and the recall [23]. Each classified theme was analyzed and the Precision, Recall, and F1 score were calculated on the test dataset. On average, the resulting scores for the classified themes across the reviews for all 50 applications were 89.4% Precision, 85.87% Recall, and 87.1% F1 Score. Table 1 shows the Precision, Recall, and F1 scores for each category.

3.6.4 Text-based Analysis of Negative Reviews. Next, we performed another text-based classification of the negative security and privacy reviews (n = 52,749) using the keywords generated in section 3.6.2 which gave us the respective distribution of these reviews based on the themes identified in section 3.6.1 as shown in Table 1. It is important to note that the review classification is not mutually exclusive, i.e., a single review can fall under multiple themes simultaneously, e.g., confidentiality, user information, and transaction.

4 RESULTS

4.1 Privacy and Security Reviews Distribution

At the end of our data preprocessing, the resulting 163,210 user privacy and security reviews from the 50 mobile payment applications were analyzed to understand the distribution of the positive and negative reviews in each of them. 52,749 (32%) comments were negative, 97,557 (60%) were positive, while we had 12,904 (8%) neutral comments. While Revolut had most number of reviews (n = 11,486) and most number of positive reviews (n = 7,211), the lowest number of reviews and positive reviews were found in Lyf Pay. Payzapp (n = 4,168) and Lyf Pay (n = 4) had the highest and lowest number of negative reviews respectively. Figure 2 below shows the distribution of positive, neutral, and negative reviews of the 50 apps. In terms of the distribution of positive and negative reviews in each of the apps, AfterPay (84%)

Table 2. Details of the Applications along with PSR (Privacy and Security Rating Score from 163, 210 Reviews) and PSNR (Privacy and Security Rating based on the 52, 749 Negative Reviews) with Counts of Negative Reviews in Account Access (AA), Confidentiality (C), Permission (P), Transaction (T), Usability (U), User Information (UI) along with Counts of Total Privacy and Security Reviews (TPSR) and Counts of Total Privacy and Security Negative Reviews (TPSNR)

Application	PSR(%)	PSNR(%)	AA	C	P	T	U	UI	TPSR	TPSNR
Affirm	70.9	30.67	150	4	3	184	250	202	4093	727
Afterpay	83.77	38.67	82	0	3	121	134	21	3320	345
BankMobile App	62.16	35.49	90	2	5	117	134	17	1030	244
Capital One Mobile	70.75	37.57	698	16	63	304	707	191	7163	1389
Cards - Mobile Wallet	44.54	29.09	48	7	2	9	70	15	348	110
CareCredit Mobile	59.2	28.89	136	2	2	23	117	31	871	225
Cash App	44.68	29.3	1825	24	33	1113	1388	480	11364	4004
Citi Mobile	77.86	42.22	512	5	5	192	538	73	5515	927
Citizens Bank Mobile Banking	43.66	30.71	854	5	8	301	864	110	3613	1354
Cointab	60.86	32.31	12	0	2	22	23	9	163	52
Credit One Bank Mobile	64.22	34.08	688	4	5	291	571	212	5200	1378
Discover Mobile	75.24	38.85	625	11	34	185	766	99	7943	1197
Ecobank Mobile App	34.09	27.88	511	8	4	284	607	97	2248	1026
eSewa	48.91	31.75	93	4	3	82	126	34	797	257
GoBank	44.61	28.15	270	2	4	165	196	52	1279	471
Google Pay	34.47	26.04	206	6	22	655	660	131	2967	1534
Green Dot	40.61	28.15	1024	8	13	547	676	234	4030	1760
IME Pay	53.58	38.5	9	1	2	14	30	15	162	40
Klarna	46.19	27.59	282	5	10	441	745	214	4511	1397
Lyf Pay	35.56	30	1	0	0	0	3	3	9	4
M&T Mobile Banking	42.74	30.1	150	3	2	68	197	10	868	305
MobiKwik	34.97	23.06	777	31	93	2038	1595	339	6874	3801
MobilePay	40.95	31.25	7	0	1	4	12	1	42	16
MoneyGram	49.45	28.6	255	5	27	216	254	70	1605	593
My Boost	60.1	36.97	296	12	23	233	686	48	5378	1623
Navy Federal Credit Union	49.41	34.47	664	3	32	436	954	79	5157	1364
Oxigen Wallet	27.19	22.6	181	3	2	584	468	80	1630	877
PayPal	44.13	28.13	1776	26	24	848	1559	511	9510	3648
PayRange	60.91	36.61	121	8	22	119	254	16	1975	484
paysafecard	47.99	29.29	41	1	3	7	31	15	273	84
Paysera Mobile Wallet	45.95	26.67	20	0	0	12	22	11	148	48
Paytm	35.78	25.28	259	10	20	475	430	111	1971	1072
Payzapp	32.97	25.87	1028	41	21	1928	2286	887	7308	4168
PREMIER Credit Card	49.36	31.86	188	2	2	60	159	34	876	322
Pyypl	35.84	23.7	48	1	0	63	94	28	447	184
Revolut	52.86	29.06	1839	48	30	811	1591	636	11486	3507
Samsung Pay	31.11	26.74	19	0	3	8	62	7	198	86
Sezzle	66.2	27.39	31	1	1	55	44	20	674	119
Shell US & Canada	37.37	26.38	56	1	9	29	107	14	448	160
Step	68.02	30.67	74	4	1	28	63	23	993	163
Suntrust Bank Mobile	52.4	33.25	497	5	14	331	716	46	4234	1226
T Wallet	37.02	28.48	32	3	2	72	73	10	262	125
tmw	34.13	22.06	120	1	1	234	215	45	824	407
U.S. Bank Mobile	69.99	40.75	530	6	10	548	864	66	6958	1494
UltraCash	62.7	36.11	5	2	2	36	37	12	237	72
Venmo	43.98	27.82	1317	285	33	1252	1647	686	9959	3755
VodaPay	28.79	23.13	18	0	0	16	51	10	214	83
Wells Fargo Mobile	57.77	33.59	1052	13	34	538	1311	136	7828	2151
Zelle	38.69	24.96	761	21	77	345	926	347	4673	1837
Zip (Quadpay)	73.68	31.72	153	1	5	180	253	71	3534	534

has the highest percentage of positive reviews and Payzapp has the highest percentage of negative reviews (57%). Based on the rating scores, AfterPay (84%) showed the highest rating score while Oxigen Wallet (27%) showed the lowest rating score.

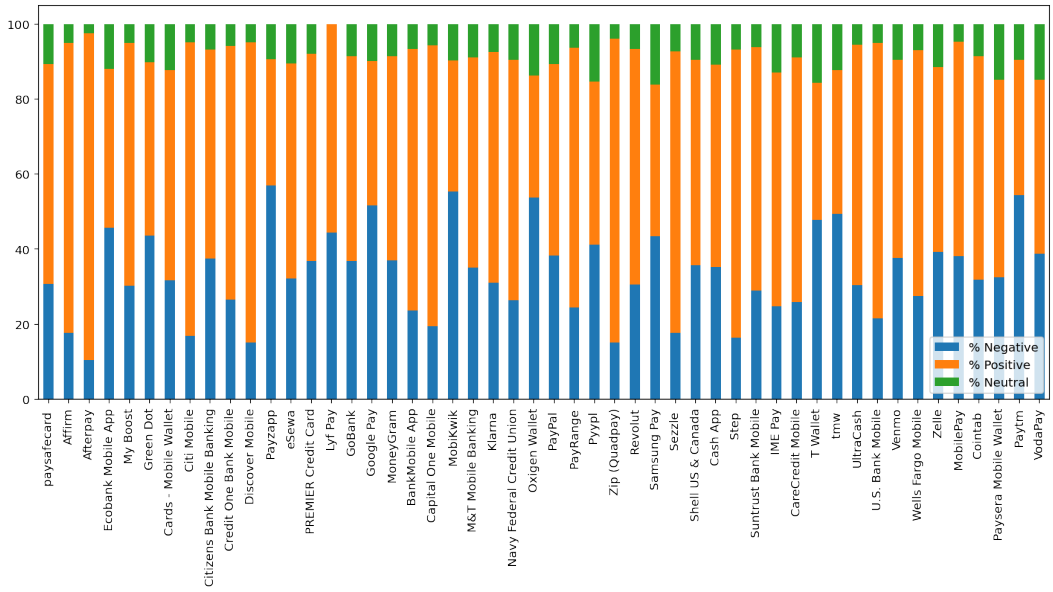

Fig. 2. Mobile Payments App Review Distribution Based on the Sentiment Analysis

4.2 Thematic Evaluation and Anecdotes

The result of our sentiment analysis showed that users tagged 52, 749 reviews as negative. Hereon, we focus on the negative reviews identified therein. A closer look at this number showed the following thematic occurrences: account access (n = 20, 431), confidentiality (n = 651), permission (n = 717), transaction (n = 16, 624) usability (n = 25, 566) and user information (n = 6, 609). The reviews are not mutually exclusive, hence a single review can have more than one theme tag. For example, the review:

> "Horrible! I literally just opened an account a few days ago because I'm going through a very rough time and someone sent me some money to help me and almost immediately my account was frozen. I have done everything asked to verify my account and still have gotten no response. Just a bunch of generic email responses. So I'm still in a bind and have no way to get the money sent to me. I just want to cry I'm so frustrated."

is tagged to be an "account access" review as the user's account is frozen, "transaction" because the user had been debited, and "user information" because the user has provided information for account verification. The most prominent concern by users remains usability issues.

Account Access: Account access tagged reviews are focused on users' need to gain legitimate access to their accounts. The highest number of account related concern was found in Revolut (n = 1, 839) covering over 9% and the lowest number was found in Lyf Pay (n = 1) as shown in Table 2. It is evident that users are concerned with accessing

their accounts in a mobile payment app as they would not be able to perform any action if they are unable to log in or have been locked out of their accounts.

Inability of users to login to their account is common among the account access concerns. For instance, the review:

> "I'm unable to login to app almost 2 years now. I have my amount 10000 which I haven't used and got stuck here. Allow me to use that. Refund the amount. Should I make any further complaint? There is no response to mails as well..."

indicates how difficult it is for the user to access their account and how they could have issues in requesting a refund of their money when they are unable to access their account.

Account lock based on scam or suspicious activity is also as another important concern of users when utilizing payment applications. Users would expect that an in-depth investigation should be performed before account access is revoked. The reviews below:

> "Be careful guys, they take part of the scammers. I had a charge back from a scammer, I provided them all the documentation that they asked for, but after that they refunded the money to the scammer, and they closed my account without any reason. So guys if you get a charge back consider that you lost the money and your account is gonna be closed without any reason."

> "My account was restricted without any previous warning, I'm on a holiday in the middle of nowhere and can't get access to my money."

shows incidents where the user is unable to access their account due to perceived suspicious activity (like scam or incorrect location).

Multi Factor Authentication (MFA) is provided to ensure the security of the mobile payment applications but this can become troublesome for some users. Consider the review:

> "what is wrong the app when i login otp is sent, the app closed auto and when i'm back i cant add the otp!"

which has usability issues combined with account access. The user is required to insert an OTP upon their login but the app closes before they could enter the OTP that was received. Another review

> "I overall love the app but lately I have had a very frustrating experience with the login. It only gives you 3 tries with your fingerprint and then locks you out and requires you to change your password. Why not first allow the user to enter their password? Also, if locked out, please make it so it is temporary instead of requiring the password change that I then have to go and update on all of my devices. Very bad UX."

indicates the concern of users when the app does not provide an alternative layer of authentication. In this case, the fingerprint failed to work thrice, and the user then got locked out of their account.

Transaction: Transactions form a core aspect of mobile payment applications. These reviews are specifically related to financial transactions which could include sending money, receiving money, making payments, and viewing account balances among other. Of the 16,624 reviews tagged as transaction-related, Mobikwik has the highest number of transaction-related concerns with over 2,038 (12%) reviews and Mobile Pay has the lowest occurrence of transaction-related concerns with only 4 reviews.

Failed transactions are the biggest concern when using a mobile payment application as they are the most reported. These failed transactions could lead to a user being debited and the recipient not credited as seen in the review below:

> "My 1000 rupees stuck in tnw wallet I tried to load in Amazon,but transaction failed but money in tmw wallet got debited, I'm going to launch FIR, guy's get ready to receive the legal notice, how careless to run away with people's money???"

is an example of a transaction that failed and the user got debited. In another form of failed transaction, it appeared the user added money on the app but were unable to complete a successful transaction as highlighted in the review

> "Very frustrating app whenever I want to purchase prepaid data it says "sorry something went wrong on our side" I don't think it works so I've uninstalled it." "fake app... DONT load money in this app.. once loaded there is no way to use the money... all the options have some error.. and finally your money is stuck. On my last review i got a response from the developer that services will be restored on 3rd week of august. Its 2nd week of september... Still no hope... Money is stuck... Please dont use this app."

Users were also displeased with bugs in app that prevented them from completing transactions due to wrong information stating that their balance was insufficient

> "Every time transaction failed with message insufficient balance...i have enough balance still same problem.....i dont have option to rate 0 otherwise i will rate 0. how much time it will take to upgrade?? Listening same answer from you since 1 months ...No prior information given about update else i will transfer my balance..... Initially deadline given was 31st july than 3rd week of august and now September started but still i cant use tmw wallet.... atleast allow us to withdraw our money....."

Double charges in transactions have also been emphasized. In certain cases, users have been charged more than once for a single transaction

> "The balance is never accurate. You can't request money without the person being double charged. Hard to navigate. and plus you have to remember to click on make it private otherwise the whole public is going to see your transactions"

Another issue that users experience is *inability to cancel wrong payments*. In the cases where users have mistakenly initiated a transaction to a wrong account, it was difficult or impossible to revert such transactions as shown in the review below:

> "Impossible to cancel payment or get money back if debit out to wrong account with same name. Just count it as a loss"

Usability: Users are cognizant of the usability of an app. In fact for mobile payments, this theme received most reviews (n = 25, 566). While the main function of a mobile payment application is to complete transactions, concerns such as unclear error messages, speed, glitches and misplaced elements can be a hindrance for users when completing these transactions. Payzapp has the most usability issues (n=2, 286) and Lyf Pay has the least usability issues (n=3).

Bugs and glitches in apps have been highlighted in multiple occasions, users have complained of app freeze especially when they want to access their accounts as highlighted in the review below;

> "Took forever to login the first time. Had to attempt multiple times. Unable to access account to make a payment. Keeps freezing after you hit the account you want to see. My personal bank is far easier to use."

> "The app is constantly disabling my biometrics in the app, even though nothing has changed with my biometrics! It's really annoying!"

> "I'm sorry, have to downgrade to 1 star, the app is constantly crashing as soon as I log in. Freezes my phone. What did you guys do now?"

Other times, these issues have been identified after *updating the application* to the current version on Play Store, as shown in the reviews below:

> "New update doesn't allow me to sign in 90% of the time and if it does let me I have to scan my finger/put in password more than once. The fact that this update has been out as long as it has with no bugs fixed shows you why wells Fargo has the horrible reputation that it does. All these bad reviews as well and still nothing...? Pathetic"

> "Not sure about this new update. My finger login keeps not working and keeps making me reset my password everyday because it's not working. I've even reset my fingerprint a few times and still. Getting ridiculous. Never use to be a problem."

> "Since my last Android update I can't even sign in! I reset the password and it immediately tells me it's incorrect. Very frustrating"

Un-intuitive interface can give users a hard time while using an application, users reacted that while navigating the app, buttons or functionalities can be hard to detect. For instance, the reviews below:

> "New app design is very difficult to navigate and does not function well. I am now forced to use online website for even simple tasks like balancing my checkbooks. Not Good."

> "The new redesign is completely and utterly terrible I don't need a search bar every time I touch the screen I need to see the numbers for incoming and outgoing funds it's a banking app not a social media app I don't care about all the pretty bells and whistles I need to see numbers and I don't need them to move every time I touch the screen I'm seriously debating changing Banks now because I cannot use this to run a business"

where the user had to leave the mobile application to use the web application and raised several concerns after an app update respectively.

User Information: User information encompasses reviews that concern the collection of personal information, user documentation, and identity verification. User verification is an important aspect of mobile payment apps but users have shown concerns as to the amount of info required for verification as well as the point at which certain verification is initiated by the app developers. We collected 6, 609 user reviews, Payzapp had the highest number of user information reviews (n = 887) while Mobile Pay had the lowest number of user information reviews (n = 1).

Users have raised concerns regarding the *inability to remove personal data* from the app when they no longer want to use the mobile app. In a review;

> "Terrible app design for something so simple. It's literally unusable yet I can't even remove my card info from this awful app, which is a major security flaw."

where a user complained about not being able to remove their card information from the app. Also, some instances of *unnecessary data collection* take place, as in the case of the review below:

> "Received Error Message - My Credit Union wasn't on the list, but the app allowed me to proceed entering all of my debit card/personal info. After submitting this information, an error message told me to contact Zelle. Turns out that if your bank isn't on Zelle's list, you can only *send* money, and I needed to receive

> funds. Zelle probably now has my name, email/home addresses, and card info floating around in some unknown server and I couldn't even finish signing up. Uninstalled."

where the user had entered all their information before being notified of a missing requirement.

Users express concern on the *introduction of limits to their transactions* by the app developers just so they could complete certain verification processes as the case of;

> "It sometimes lock my deposit, because I cannot receive SMS messages from their side. They use limits for deposit, I cannot remove them, because you need make videocall for identification. Operator said that my connection bad and cannot help me. Scammers"

and cases where *change in user info* such as phone number could affect their access to the application;

> "I have changed cellphone but unable to register with same phone number on new mobile..."

Confidentiality: While using mobile payment applications, a lot of user information is being utilized and transactions are recorded. Users have shown concerns about revealing personal information to third-parties. However, confidentiality-tagged reviews are the lowest (n = 651). Unsurprisingly, 43% of the confidentiality tagged reviews are attributed to Venmo. This is because the app is known to publicize users' transactions by default. The review;

> "The balance is never accurate. You can't request money without the person being double charged. Hard to navigate. and plus you have to remember to click on make it private otherwise the whole public is going to see your transactions. That shouldn't even be a thing. However, there are several people that I have to trade money back and forth with that use Venmo, so I have to use it and hope for improvement."

highlights a commenter's concern on the sharing of their transactions with the public when using Venmo.

Commenters also share concerns on *data being shared with third-parties* and *inadvertent keeping of user's information* as highlighted by the comments below respectively;

> "Paytm shared our data with Chinese firms, now paytm lossing our trust very badly time to uninstall this APP"

> "Broken and gives vague error message. Customer support is nonexistent. Dont bother with this. Let me also add they dont actually delete your private info when you erase your account, so if you are tired of companies exploiting your info then very very much avoid this app..."

Permission: Mobile payment applications require specific permissions to perform certain operations on a user's device. We collected 717 permission-related reviews. It is expected that users raising permission concerns are technologically savvy, at least to a certain degree. Mobikwik showed most permission concerns with over 93 reviews tagged. In terms of permission, most concerns can be attributed to *perceived unnecessary permissions* requested by mobile payment applications. Some applications request access for permission to access mobile data or functionality that raises concerns to the user. For instance, the following reviews;

> "This app needs 'send and view SMS' permission to send SMS only. I think send SMS permission is quite enough for the same, isn't it? Correct me if I'm wrong."

> "Due to privacy concerns, I've uninstalled the app from initial opening screen of the app due to nonsensical permissions. I just want it to have one permission, send and receive messages for the OTP."

> "New update requires permission to view device use including what other apps are running, history, and bookmarks. Why does a card payment app need this extra information? Spyware? No thanks."

highlight some concerns that the commenters have raised regarding permissions being requested.

In other cases, users grant mobile payment applications but they still don't function as expected as expressed by a commenter;

> "It's the worst app ever, even after giving location permission it is still asking to give location permission"

4.3 Application Performance

4.3.1 Top 5 Apps with Highest PSR. We determined the performance of the mobile payment applications based on their respective PSR scores (as explained in section 3.5). The apps with top 5 PSR scores are: Afterpay (84%), Citi Mobile (78%), Discover (75%), Zip (Quadpay) (74%) and Affirm (71%). Notably, Afterpay, Citi Mobile and Discover have more than $5M$ downloads. Figure 3 shows the distribution of the themes in each application for the applications with the highest PSR. The numbers below are for negative privacy- and security-related reviews.

Afterpay had no confidentiality tagged reviews and only 3 permission tagged reviews from a total of 345 reviews. However, the app has 134 usability tagged reviews, one of which is;

> "Irritated, why aren't biometrics working at all and then when using a password in app it keeps saying "something went wrong" and one got to try over and over again."

Account access concerns were trailing with a count of 82 reviews.

Citi Mobile had a total of 927 reviews and only had 5 reviews each for confidentiality and permission. Usability issues are leading as well with a total 538 followed by account access issues (n = 512). One usability review by a commenter below is an example;

> "Such an awful experience. Worked fine for a week. Now constantly having "temporary delays" and after a few attempts it locks my account for 24 hours, three days in a row. Trying to reset my password and getting the message that the data I enter doesn't match the banks records, which is not true and confirmed by a manager during a call. Is a result - no online banking at all. Can't even check my balance."

Discover also showed most issues as usability (n = 766) and account access (n = 625) targeted while confidentiality remained lowest at 11 reviews only out of a total of $1,197$ reviews. One of the usability issues that have the user complaining of the app's functionality mentions:

> "This app consistently doesn't work for me when I try to use its noble check deposit feature. Despite trying to use this feature at various times during business (and non-business) hours, I often receive the following message: "Some of our web features are not available at this time." Is a result, I must deposit my checks at a bricks-and-mortar bank. Disappointing, frustration, annoying, time-wasting."

Zip [5] has a total of 534 reviews and usability concerns are highest (n = 253) which is followed by transaction-related concerns (n = 180). Only 1 review was tagged as confidentiality.

Affirm has a total of 727 reviews dominated by 250 usability concerns and 202 user info concerns. An example of a review that falls into account access, usability, user info, and transaction would be;

> "You cannot update contact information without being locked out of your account for weeks at a time. Verified identity, updated phone number. It has been 3 weeks still nothing has been done. Cannot use account. This app is useless after first purchase is paid off. It locks your account and lowers your spending limit."

[5] Zip was formerly called Quadpay.

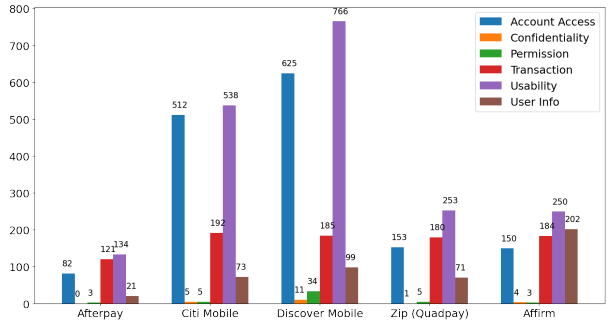

Fig. 3. Number of Reviews Analyzed for the Apps with the Highest PSR

4.3.2 Bottom 5 Apps with Lowest PSR. The 5 apps with the lowest PSR scores are: Ecobank (34%), Payzapp (33%), Samsung Pay (31%), Vodacom (29%) and Oxigen Wallet (27%). Figure 4 shows the distribution of the themes in each application for the applications with the lowest PSR. The numbers below are for negative privacy- and security-related reviews.

Ecobank showed 607 usability and 511 account access issues from a total of 1, 026 reviews. An example of usability concern by a commenter is;

> "For the past two months, when I changed my phone, this app has refused to recognise my number. I've just been wasting my data on downloading and install"

Payzapp showed 2, 286 usability, 1, 928 transaction, and 1, 028 account access issues from a total of 4, 168 reviews. Such as;

> "I tried to load money to my wallet. But it showed failed. But i got message from bank that money has been deducted. I sent an mail on this issue. But nothing happened."

Samsung Pay had a total of 82 reviews which is dominated by usability concerns (n = 62). Such as;

> "Samsung pay forces you to set a lock in your watch (SG4)... That doesn't sound so stupid until you realize you pay with Samsung once a day and you have to lock your screen 100 times a day to see anything. But a lock screen of THE APP! That was how it worked in previous watch SG3, should take minimum effort."

Vodapay had a total of 83 reviews with 62 usability concerns. One of the examples for the reviews tagged as "usability" includes:

> "The app is really useless to me. It only works at the time you download it after that it freeze and says you must pull down to refresh but nothing happens when you pull down the page."

Oxigen Wallet had a total 468 and 584 usability and transaction tagged reviews respectively from 877 total reviews. It has only 2 permission concerns and 3 confidentiality concerns. One of the user mentioned:

> "Oops, something went wrong, try after some time. This is what I get as soon as I launch the app. Fix it."

5 DISCUSSION

In our research, we implemented mixed-methods to analyze user-generated reviews on the privacy and security of mobile payment applications. We collected the reviews of top 50 mobile payment applications with at least $1M$

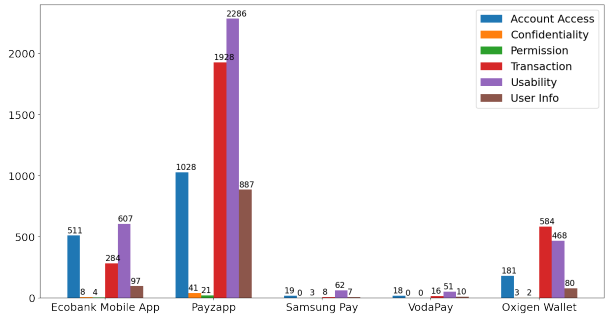

Fig. 4. Number of Reviews Analyzed For The Apps with the Lowest PSR

downloads and performed our analysis through sentiment analysis to identify the negative privacy- and security-related reviews. The resulting reviews were coded thematically into six themes; account access, usability, transaction, user information, confidentiality, and permission.

From the sentiment analysis, we note that of the total, 97, 557 (60%) reviews had a positive sentiment and 52, 749 (32%) reviews had negative sentiment across all the collected reviews from the 50 mobile payment application. Recall that, we calculated the app ratings provided by the users who gave privacy and security ratings and those who gave negative reviews from the privacy and security lenses (refer section 3.5). The PSR scores across the applications ranged from as high as 83.77% in the case of Afterpay and as low as 27.19% in the case of Oxigen Wallet.

Since users tend to leave longer and more detailed negative reviews [59], we performed an in-depth study focusing on the negative reviews. Based on our findings, we found that usability is the most reported concern by users. About half of the negative privacy and security reviews were related to usability (48%). Users struggle to complete actions while using mobile payment applications due to bugs and glitches, unclear error messages, and a non-appealing user interface. In particular, users had complained about issues caused by app updates indicating that in some cases, functionalities stopped working when they updated the application.

One of the essential functions of mobile payment applications is to complete transactions; however, to achieve that goal, the application must have a limited number of usability barriers while causing minimum hindrance for legitimate users who request access to their accounts. The results show that account access is another primary concern for users. Users are terrified when they cannot access their own money due to policies by specific mobile payment applications. Although scam and suspicious activities cannot be entirely mitigated in the use of mobile payment applications [10] users are still unclear as to actions that could lead to account lock or suspicious activities. Account access concerns covered 39% of the negative privacy and security reviews.

Investigating the core functionality of mobile payment applications, i.e., performing financial transactions which covered 32% of the reviews, it was clear that mobile payment applications still struggle to distinguish between a successful and an unsuccessful transaction, especially in the case where two different parties are completing transactions. Users mostly complained of failed transactions where users are debited, and the recipient never got credited, and it takes much time and back and forth to reconcile these faulty payments. While noting that users can make mistakes, another major issue that users experience is the inability to cancel a wrong transaction. Here, the critical question remains: what happens when a user sends money to the wrong person? This is especially important when transactions have been simplified to the extent that just the mobile number of the recipient is enough to complete a transaction.

User information, which covered 13% of the negative privacy and security reviews, reflects users' concern regarding the personal information requested while using mobile payment applications. In some instances, mobile payment applications collect too much information from users before giving them specific access when using the applications. Users are furious if they have to give all their information only for them to be declined in the end. The critical question here is: what is the minimum amount of information an application should request from a user to provide the minimum viable access for them to use the application? Another huge concern for users is what happens to their information when they decide not to continue using a mobile payment application.

Permission (1.4%) and confidentiality (1.2%) are less concerning, understandably, because they do not affect the overall functioning of the mobile payment application in most cases. However, some technical know-how is required to take note of permissions requested by an application. During app development, research has shown that developers sometimes request dangerous and unnecessary permissions, which could raise users' suspicion [26]. For confidentiality, certain users are concerned about their transactions or personal information being accessed by third-parties. Ideally, transactions should be private by default unless specified otherwise by users [8]. It is thus essential to keep these aspects on the radar.

6 IMPLICATIONS AND RECOMMENDATIONS

Our findings shed light on the user perception of mobile payment applications from the privacy and security perspective. Based on our findings, we propose the following recommendations to improve the privacy and security of mobile payment applications.

Robust Account Access & Authentication: The seamless integration of mobile payment applications cannot be over-emphasized. However, many reviews indicated concerns about third-party access or getting locked out of their account. Thus, as in prior work, we recommend robust authentication and access control [62]. This may involve introducing more user-centered authentication mechanisms to aid users' account access and provide multiple avenues of verifying their identity, which should not lock them out of their accounts. For instance, an app could have both fingerprint and password options for a user to log in to their account and use the one they prefer. In addition, multi-factor authentication (MFA) is an essential aspect of mobile payment applications [29] but in some cases could lead to unwanted usability issues for the users [35]. Therefore, a good balance must be found for both MFA and usability as suggested in prior works [15, 38].

Fixing Usability Issues: Usability issues have continuously been reported [39] in the use of mobile payment applications in prior works and our reviews. App developers need to employ usability tests when deploying new functionalities. It is also important to test existing functionalities to ensure that new functionalities do not impair their performance, as is done in regression testing. Developers' implementation of privacy and security is studied where these robust mechanisms focusing on the user side are mentioned [2, 65]. We must ensure accountability on the development side; every app goes through auditing and proper tests before deployment. Especially with more apps originating every day, design challenges must be addressed for seamless and successful integration with financial organizations. Additionally, usability guidelines developed through prior work [45, 54, 55] and experts should also be applied to these mobile payment applications.

Limiting User Information Request, Storage, and Sharing: User information is needed for account verification in almost all mobile payment applications. However, minimum viable information should be required to verify users, and users should not have to share all their information before the decision to approve or disapprove their account is provided. Also, users should be able to request the deletion of their personal information from mobile payment

applications when they no longer use them. The European General Data Protection Regulation (GDPR) helps in this regard, but the process remains less simplified for users [58]. In the same way, users' data and transaction records to third-parties need to be looked into holistically. Sharing user data by default is a significant concern, especially for users that are not technically savvy, as in the case of Venmo [8]. Finally, app developers should only request permissions that are pivotal to performing operations in the app [48]. This would ensure that users are not skeptical of using payment applications.

Accountability and Fraud Detection: In terms of an unsuccessful transaction, given that it is the fundamental functionality of the mobile payment applications, due to obvious reasons, many app users complain if the transaction was not successful or a fraudulent transaction went through. Ensuring secure payment through the application is a priority that proper authentication should first handle. After that, we can implement MFA techniques such as OTP every time a transaction is generated [29, 44]. Moreover, if a fraudulent charge is generated, we can verify with the user via proper channels such as emails. All these fail-safe mechanisms still do not ensure 100% security; thus, there should be proper customer support who can help their users, especially when it comes to digital payments.

App Level Regulations: Regulations such as the Fair Information Practice Principles (FIPP) and the General Data Protection Regulation (GDPR) form guidelines for privacy policies [67]. Although there has been a moderate positive impact on application privacy with fewer declared permissions and lesser user concerns across Android applications after the introduction of GDPR [43], there is still a gap overall and lack of support for developers in implementing such policies in practice [16]. The same is reflected in the security domain where developers may be aware of the security best practices, such as those outlined by Android [25], but lag when it comes to implementation, especially in the case of smaller companies [6, 64]. Thus, we propose to implement these policies at an app level with regular auditing to ensure the effectiveness of these policies. Additionally, proposals for stricter regulations can be made to prevent fraudulent activities for digital transactions.

7 LIMITATIONS AND FUTURE WORK

Mobile payment applications have been reported to be vulnerable by users through their generated reviews. Users have shown concerns about breaches, exposure of information, and failed transactions, however, given the limitation of the work, the actual security and privacy evaluation of the applications is not done from the code analysis perspective. This was outside of the scope of this work. To complement these findings, we would introduce a comprehensive static and dynamic analysis of mobile payment applications as a future extension. Additionally, we removed emojis and emoticons because of the inefficiency of available dictionaries to convert them into textual content; however, we believe supplementing emojis and emotions as additional features can contribute to the sentiment of the reviews. Also, we collected our thematic topics for privacy and security reviews through manual coding of the reviews. As a future extension, we would focus on topic modeling techniques such as Latent Dirichlet Allocation (LDA) to discover abstract topics that occur in our collection of documents. We would perform sentiment classification using sentence-level lexical-based semantic orientation to evaluate the subjectivity of reviews at the sentence level.

8 CONCLUSION

Mobile payment applications have gained popularity in the last few years due to their accessible nature for quick digital transactions. However, this has given rise to several privacy and security concerns. Prior research has focused on the technical evaluation of these applications. It is critical to understand the user perception of these applications as they are the entities using them. To this aim, we collected a total of 1, 886, 352 app reviews from the top 50 mobile payment

applications of the Google Play Store. After that, we extracted 163, 2103 privacy- and security-related reviews and analyzed the 52, 749 negative reviews through manual and automated analysis. We realized that there exist an array of privacy and security-related concerns highlighted by users, which include; account access (38.73%), digital transaction completion issue (31.52%), and permission model of the application (13.60%), and others. We also noticed some usability (48.47%) concerns that generate privacy and security issues as users use these applications in their daily lives. While the primary use of such an app is to complete a transaction, usability concerns which focus on the ability to use the app to perform operations, and account access concerns which focus on the ability to access one's account legitimately, remain the most concerning for users when using these applications. Finally, we provide actionable recommendations regarding the possible ways to mitigate the issues identified through this research.

9 ACKNOWLEDGEMENT

We want to thank the initial contribution of Karin Mortl (Ph.D. Student, University of Denver), who started the project focusing on Venmo as a case study. We would also like to acknowledge the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Lab at the University of Denver, where this research was conducted. Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors.

REFERENCES

[1] Aijn Abraham, D Schlecht, G Ma, M Dobrushin, and V Nadal. 2016. Mobile security framework (MobSF).

[2] Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. 2016. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. *2016 IEEE Cybersecurity Development (SecDev)* (2016), 3–8.

[3] Shivani Agarwal, Mitesh Khapra, Bernard Menezes, and Nirav Uchat. 2007. Security issues in mobile payment systems. *Computer Society of India* (2007), 142–152.

[4] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 787–796.

[5] Yoris A Au and Robert J Kauffman. 2008. The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic commerce research and applications* 7, 2 (2008), 141–164.

[6] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason I Hong, and Lorrie Faith Cranor. 2014. The privacy and security behaviors of smartphone app developers. (2014).

[7] Zlatko Bezovski. 2016. The future of the mobile payment as electronic payment system. *European Journal of Business and Management* 8, 8 (2016), 127–132.

[8] Monica Caraway, Daniel A Epstein, and Sean A Munson. 2017. Friends don't need receipts: The curious case of social awareness streams in the mobile payment app Venmo. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–17.

[9] Lei Cen, Deguang Kong, Hongxia Jin, and Luo Si. 2015. Mobile app security risk assessment: A crowdsourcing ranking approach from user comments. In *Proceedings of the 2015 SIAM International Conference on Data Mining*. SIAM, 658–666.

[10] Ramesh Chandran, S Rakesh Kumar, and N Gayathri. 2021. Designing a locating scams for mobile transaction with the aid of operational activity analysis in cloud. *Wireless Personal Communications* 117, 4 (2021), 3015–3028.

[11] Cybercrimemag. 2021. Cybercrime to cost the world 10.5 trillion annually by 2025. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[12] Tomi Dahlberg, Niina Mallat, Jan Ondrus, and Agnieszka Zmijewska. 2008. Past, present and future of mobile payments research: A literature review. *Electronic commerce research and applications* 7, 2 (2008), 165–181.

[13] Sanchari Das, Andrew Dingman, and L Jean Camp. 2018. Why Johnny doesn't use two factor a two-phase usability study of the FIDO U2F security key. In *International Conference on Financial Cryptography and Data Security*. Springer, 160–179.

[14] Sanchari Das, Robert S Gutzwiller, Rod D Roscoe, Prashanth Rajivan, Yang Wang, L Jean Camp, and Roberto Hoyle. 2020. Humans and technology for inclusive privacy and security. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 64. SAGE Publications Sage CA: Los Angeles, CA, 461–464.

[15] Sanchari Das, Bingxing Wang, Zachary Tingle, and L Jean Camp. 2019. Evaluating User Perception of Multi-Factor Authentication: A Systematic Review. In *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*.

[16] Jose M Del Alamo, Danny Guaman, Belen Balmori, and Ana Diez. 2021. Privacy Assessment in Android Apps: A Systematic Mapping Study. *Electronics* 10, 16 (2021), 1999.

[17] Jayati Dev, Sanchari Das, and Linda Jean Camp. 2018. Privacy Practices, Preferences, and Compunctions: WhatsApp Users in India.. In *HAISA*. 135–146.

[18] Yvonne D Eaves. 2001. A synthesis technique for grounded theory data analysis. *Journal of advanced nursing* 35, 5 (2001), 654–663.

[19] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14.

[20] Denzil Ferreira, Vassilis Kostakos, Alastair R Beresford, Janne Lindqvist, and Anind K Dey. 2015. Securacy: an empirical investigation of Android applications' network usage, privacy and security. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 1–11.

[21] Elizabeth Fife and Juan Orjuela. 2012. The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management* 4, Godište 2012 (2012), 4–11.

[22] Barbara L Filkins, Ju Young Kim, Bruce Roberts, Winston Armstrong, Mark A Miller, Michael L Hultner, Anthony P Castillo, Jean-Christophe Ducom, Eric J Topol, and Steven R Steinhubl. 2016. Privacy and security in the era of digital health: what should translational researchers know and do about it? *American journal of translational research* 8, 3 (2016), 1560.

[23] Peter Flach and Meelis Kull. 2015. Precision-recall-gain curves: PR analysis done right. *Advances in neural information processing systems* 28 (2015).

[24] Xiang Gong, Kem ZK Zhang, Chongyang Chen, Christy MK Cheung, and Matthew KO Lee. 2019. What drives self-disclosure in mobile payment applications? The effect of privacy assurance approaches, network externality, and technology complementarity. *Information Technology & People* (2019).

[25] Android Developers Guide. [n.d.]. App Security Best Practices: Android Developers. https://developer.android.com/topic/security/best-practices

[26] Hongmu Han, Ruixuan Li, and Xiwu Gu. 2016. Identifying malicious Android apps using permissions and system events. *International Journal of Embedded Systems* 8, 1 (2016), 46–58.

[27] Yijun Huang and Wenwen Liu. 2012. The impact of privacy concern on users' usage intention of mobile payment. In *2012 International Conference on Information Management, Innovation Management and Industrial Engineering*, Vol. 3. IEEE, 90–93.

[28] Johannes Huebner, Remo Manuel Frey, Christian Ammendola, Elgar Fleisch, and Alexander Ilic. 2018. What people like in mobile finance apps: An analysis of user reviews. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*. 293–304.

[29] Jesús Téllez Isaac and Zeadally Sherali. 2014. Secure mobile payment systems. *It professional* 16, 3 (2014), 36–43.

[30] Vess L Johnson, Angelina Kiser, Ronald Washington, and Russell Torres. 2018. Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior* 79 (2018), 111–122.

[31] Monisha Kanakaraj and Ram Mohana Reddy Guddeti. 2015. Performance analysis of Ensemble methods on Twitter sentiment analysis using NLP techniques. In *Proceedings of the 2015 IEEE 9th international conference on semantic computing (IEEE ICSC 2015)*. IEEE, 169–170.

[32] Mubasher Khalid, Muhammad Asif, and Usman Shehzaib. 2015. Towards improving the quality of mobile app reviews. *International Journal of Information Technology and Computer Science (IJITCS)* 7, 10 (2015), 35.

[33] Mubasher Khalid, Usman Shehzaib, and Muhammad Asif. 2015. A Case of Mobile App Reviews as a Crowdsource. *International Journal of Information Engineering & Electronic Business* 7, 5 (2015).

[34] Burhan Ul Islam Khan, Rashidah F Olanrewaju, Asifa Mehraj Baba, Adil Ahmad Langoo, and Shahul Assad. 2017. A compendious study of online payment systems: Past developments, present impact, and future considerations. *International journal of advanced computer science and applications* 8, 5 (2017).

[35] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M Angela Sasse. 2015. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. *arXiv preprint arXiv:1501.04434* (2015).

[36] Francisco Liébana-Cabanillas, Francisco Muñoz-Leiva, and Juan Sánchez-Fernández. 2018. A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment. *Service Business* 12, 1 (2018), 25–64.

[37] Yu-Cheng Lin. 2015. Androbugs framework: An android application security vulnerability scanner. *Blackhat Europe* 2015 (2015).

[38] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. 2020. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication.. In *IEEE Symposium on Security and Privacy*. 268–285.

[39] Hafiz Abid Mahmood Malik, Abdulhafeez Muhammad, and Usama Sajid. 2021. Analyzing Usability of Mobile Banking Applications in Pakistan. *Sukkur IBA Journal of Computing and Mathematical Sciences* 5, 2 (2021), 25–35.

[40] Niina Mallat. 2007. Exploring consumer adoption of mobile payments–A qualitative study. *The Journal of Strategic Information Systems* 16, 4 (2007), 413–432.

[41] Stuart McIlroy, Nasir Ali, Hammad Khalid, and Ahmed E Hassan. 2016. Analyzing and automatically labelling the types of user issues that are raised in mobile app reviews. *Empirical Software Engineering* 21, 3 (2016), 1067–1106.

[42] Alessio Merlo and Gabriel Claudiu Georgiu. 2017. Riskindroid: Machine learning-based risk analysis on android. In *Ifip international conference on ict systems security and privacy protection*. Springer, 538–552.

[43] Nurul Momen, Majid Hatamian, and Lothar Fritsch. 2019. Did app privacy improve after the GDPR? *IEEE Security & Privacy* 17, 6 (2019), 10–20.

[44] Seema Nambiar, C-T Lu, and Lily R Liang. 2004. Analysis of payment transaction security in mobile commerce. In *Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, 2004. IRI 2004.* IEEE, 475–480.

[45] Fatih Nayebi, Jean-Marc Desharnais, and Alain Abran. 2012. The state of the art of mobile application usability evaluation. In *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 1–4.

[46] Naheem Noah, Sommer Shearer, and Sanchari Das. 2022. Security and Privacy Evaluation of Popular Augmented and Virtual Reality Technologies. In *Proceedings of the 2022 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering (IEEE MetroXRAINE 2022)*.

[47] Abu Saleh Md Noman, Sanchari Das, and Sameer Patil. 2019. Techies against Facebook: understanding negative sentiment toward Facebook via user generated content. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–15.

[48] Sai Teja Peddinti, Igor Bilogrevic, Nina Taft, Martin Pelikan, Úlfar Erlingsson, Pauline Anthonysamy, and Giles Hogben. 2019. Reducing permission requests in mobile apps. In *Proceedings of the internet measurement conference*. 259–266.

[49] Minh Vu Phong, Tam The Nguyen, Hung Viet Pham, and Tung Thanh Nguyen. 2015. Mining user opinions in mobile app reviews: A keyword-based approach (t). In *2015 30th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE, 749–759.

[50] Nikolaos Polatidis and Christos K Georgiadis. 2013. Mobile recommender systems: An overview of technologies and challenges. In *2013 Second International Conference on Informatics & Applications (ICIA)*. IEEE, 282–287.

[51] Sören Preibusch, Thomas Peetz, Gunes Acar, and Bettina Berendt. 2016. Shopping for privacy: Purchase details leaked to PayPal. *Electronic Commerce Research and Applications* 15 (2016), 52–64.

[52] Rahime Belen Saglam, Jason RC Nurse, and Duncan Hodges. 2022. Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications* 66 (2022), 103163.

[53] Zakaria Sahnoune, Esma Aïmeur, Ghada El Haddad, and Rodrigue Sokoudjou. 2015. Watch your mobile payment: an empirical study of privacy disclosure. In *2015 IEEE Trustcom/BigDataSE/ISPA*, Vol. 1. IEEE, 934–941.

[54] Maria Shitkova, Justus Holler, Tobias Heide, Nico Clever, and Jörg Becker. 2015. Towards usability guidelines for mobile websites and applications. (2015).

[55] Nadiah Mohamad Sofian, Ahmad Sobri Hashim, and Wan Fatimah Wan Ahmad. 2018. A review on usability guidelines for designing mobile apps user interface for children with autism. In *AIP conference proceedings*, Vol. 2016. AIP Publishing LLC, 020094.

[56] Statista. [n.d.]. Digital payments - worldwide: Statista market forecast. https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide

[57] Chuanqi Tao, Hongjing Guo, and Zhiqiu Huang. 2020. Identifying security issues for mobile applications based on user review summarization. *Information and Software Technology* 122 (2020), 106290.

[58] Welderufael B Tesfay, Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, and Jetzabel Serna. 2018. PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation. In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*. 15–21.

[59] Rajesh Vasa, Leonard Hoon, Kon Mouzakis, and Akihiro Noguchi. 2012. A preliminary analysis of mobile app user reviews. In *Proceedings of the 24th Australian computer-human interaction conference*. 241–244.

[60] Silas Formunyuy Verkijika and Brownhilder Ngek Neneh. 2021. Standing up for or against: A text-mining study on the recommendation of mobile payment apps. *Journal of Retailing and Consumer Services* 63 (2021), 102743.

[61] Timothy Vidas, Nicolas Christin, and Lorrie Cranor. 2011. Curbing android permission creep. In *Proceedings of the Web*, Vol. 2.

[62] Yong Wang, Christen Hahn, and Kruttika Sutrave. 2016. Mobile payment security, threats, and challenges. In *2016 second international conference on mobile and secure services (MobiSecServ)*. IEEE, 1–5.

[63] Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, and Michalis Faloutsos. 2012. Permission evolution in the android ecosystem. In *Proceedings of the 28th Annual Computer Security Applications Conference*. 31–40.

[64] Xuetao Wei and Michael Wolf. 2017. A survey on HTTPS implementation by Android apps: issues and countermeasures. *Applied Computing and Informatics* 13, 2 (2017), 101–117.

[65] Charles Weir, Ben Hermann, and Sascha Fahl. 2020. From needs to actions to secure apps? the effect of requirements and developer practices on app security. In *29th USENIX Security Symposium (USENIX Security 20)*. 289–305.

[66] Qianwen Yang, Xiang Gong, Kem ZK Zhang, Hefu Liu, and Matthew KO Lee. 2020. Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management* 52 (2020), 102065.

[67] Razieh Nokhbeh Zaeem, Ahmad Ahbab, Josh Bestor, Hussam H Djadi, Sunny Kharel, Victor Lai, Nick Wang, and K Suzanne Barber. 2022. PrivacyCheck v3: Empowering Users with Higher-Level Understanding of Privacy Policies.. In *WSDM*. 1593–1596.

[68] Hengshu Zhu, Hui Xiong, Yong Ge, and Enhong Chen. 2014. Mobile app recommendations with security and privacy awareness. In *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*. 951–960.

Table A1. Privacy and Security Keywords

Category	Keywords
Primary Keywords	private, confidential, privacy, confidentiality, secure, security, safe, personal information, access, risk, risky, scam, unsafe, steal, stole, fraud, protect, protection, breach, security, phish, spyware, malware, hack, virus, spam, leak, permission, read calendar, write calendar, read messages, intrusive, malicious, invade, safety, disclose, violate, lock, unlock, password, fake, theft
Secondary Keywords	account, transaction, credit, debit, card, advertisement, bluetooth, calendar, contact, location, mail, camera, files, network, phone, phone call, call, internet, information, data, identity, app, payment, money
Addendum Keywords	drain, block, lock, close, freeze, crash, shut, hang, stuck, glitch, laggy, stall, crush, scrape, fail, recover, trust, sketchy, limit, easy, wrong, lost, change, check, monitor, track, turn off, false, shut, misleading, intercept, verify, deny, prove, lose, harvest

Table A2. Theme Keywords

Theme	Keywords
Account Access	blocked, lock, locks, locked, locking, password, log in, log into, log on, log onto, log off, log of, login, logs me in, log me in, sign in, signed in, signin, logging, new account, hacked, can't check my account, cant check my account, can not check my account, can't get into my account, cant get into my account, can not get into my account, get in, credentials, closed, register, unable to go in, unable to get in, suspended, open account, open an account, verify my account, verify account, limit my account, limiting my account, identity theft, permanently, old number, old phone number, old mobile number, recover, recovering, create account, create my account
Confidentiality	database, everyone can, private, public, privacy, leak
Permission	permissions, location, media, gps
Transaction	transaction, transactions, transfer, transfers, transferred, purchase, purchased, purchases, paying, vendor, merchant, pmt, merchandise, deposit, deposits, deposited, funds, fund, spend, refund, refunded, charge, charged, wallet, pending, recharge, recharges, recharged, debited, credited, declined
Usability	doesnt come, doesn't come, does not come, doesnt even come, doesn't even come, does not even come, doesnt show, doesn't show, not showing, doesnt even show, doesn't even show, does not even show, not even showing, doesnt appear, doesn't appear, does not appear, not appearing, doesnt even appear, doesn't even appear, does not even appear, not even appearing, doesn't work, does not work, doesnt even work, doesn't even work, does not even work, cannot load, can not load, can't load, cannot even load, can not even load, can't even load, doesnt load, doesn't load, does not load, doesnt even load, doesn't even load, does not even load, wont load, won't load, would not load, will not load, wont even load, won't even load, would not even load, will not even load, loading, error, errors, link, slow, slowing, slowness, slows, button, freezing, freezes, glitch, glitches, glitching, glitched, bug, crash, crashes, message, ui, ux, gui, interface, gone wrong, went wrong, code, updating, update, network issue, network issues, connection issue, connection issues, forever, maintenance, decimal, buffer, buffers, buffering, nothing works, notification, notifications, not getting, fix, remember, click, clicked, tap, accessible, screen, feature, features, clunky, cache, keeps refreshing, keep refreshing, connect, connecting, connection, reminder, automatically, layout, lag, lagging, lagged, otp, delay, delays, difficult to use, not easy to to use, graphics, installed, installing, close app, 5g, 5gs, 4g, 4gs, shut down, shuts, shutting down, browser, desktop, something is wrong, technical, battery, timed out, display, unavailable
User Information	license, passport, documents, document, mismatch, my information, my info, your information, personal information, personal info, bank statement, banking information, banking info, card detail, card details, card number, card #, sensitive, kyc, my contact, tax number, tax id, medicare, birthday, birth date, date of birth, dob, social security number, ssn, identity, identify, identification, credit score, selfie