Citizens' Report on Bharat Financial Technical Glitch / Consent Scam

15 March 2022

Index

Executive Summary

In November 2021, a whistleblower report accused Bharat Financial Inclusion Limited (BFIL), an IndusInd bank microfinance subsidiary, of evergreening loans to subvert true NPA numbers. The bank admitted to having issued 84000 loans without consent of consumers and cited ‘Technical Glitch’ which prevented OTP consent to be bypassed. It said the glitch was rectified in 2 days.

While the external auditor report is awaited, this draft of citizens’ report details the issue, investigating into the matter from publicly available artefacts to document the case and present its findings.

It also makes a series of recommendations to multiple stakeholders to handle such situations in future and protect consumers from any systemic failures, technical / intentional.

1. Introduction

India has gone through rapid digitisation in the past decade led by digitisation in financial services anchored by fintechs using mobile and digital identity. *JanDhan-Aadhaar-Mobile* / *JAM trinity*, is often said to be a key enabler for financial inclusion[1] in increasing access to formal credit, specifically to the new-to-credit population. While digitisation might seemingly lower the cost for market players in delivery of financial services, particularly digital credit, the consumer harms arising out of digitised financial services get overshadowed / underreported, unless they are too large to miss.

Background

While consumer harms can be of many kinds and data privacy, credit profiling, algorithmic scoring etc usually attract attention and get widely discussed, harms arising out of consent design in systems do not get sufficient attention. **Consent Scams** are those where consumers of digital financial services get shortchanged through lack of proper consent collection by financial service providers either willfully / due to 'technical glitches'.

India has been witnessing consent scams by various digital financial service providers, all of which involved actions by providers / operators to perform transactions bypassing consent in letter / spirit. Some examples are opening of payments bank account and diverting state subsidies without knowledge of person[2], dumping a loan for attending free coaching classes offline[3] or online courseware[4]. The 'aggressive' marketing practises of ed-tech firm Byjus of dumping consent-less loans without recourse[5] was highlighted in parliament 2 years after it was first reported.

The latest to have joined the list is Bharat Financial Inclusion Limited (previously SKS Microfinance Limited), a subsidiary of IndusInd Bank (NSE:INDUSINDBK) which admitted[6] to have disbursed 84,000 loans in May 2021 without the customer consent getting recorded owing to a ***Technical Glitch*** at the time of loan disbursement while denying the allegations of evergreening. Bharat Financial incidentally also happened to be the first microfinance market player to have completely digitised their operations through Aadhaar based authentication as early as 2017[7]

---

[1] Prabhat Labh, 'Full Financial Inclusion in India? How the 'JAM Trinity' Can Help Businesses Make it a Reality' (*NextBillion,* 18 July, 2018) https://nextbillion.net/full-financial-inclusion-in-india-how-the-jam-trinity-can-help-businesses-make-it-a-reality/

[2] Anand Venkatanarayanan and Srikanth Lakshmanan, 'Aadhaar Mess: How Airtel Pulled Off Its Rs 190 Crore Magic Trick' (*The Wire,* 21 December 2017) https://thewire.in/banking/airtel-aadhaar-uidai

[3] Harsimran Julka, 'The dangers of instant Aadhaar authentication for India's 1-minute loan market' (*Money Control,* 01 March, 2018) https://www.moneycontrol.com/news/business/startup/the-dangers-of-instant-aadhaar-authentication-for-indias-1-minute-loan-market-2519013.html

[4] Olina Banerji, Arundhati Ramanathan, Rohin Dharmakumar, 'The making of a loan crisis at Byju's' (*The Ken*, 27 May 2019) https://the-ken.com/story/the-loan-crisis-at-byjus

[5] Nishant Kauntia, 'Byju's predatory practises flagged in Parliament by MP Chidambaram' (*Medianama,* 14 December 2021) https://www.medianama.com/2021/12/223-byjus-loan-sharks-mp-chidambaram/

[6] 'Clarification on news article' (*IndusInd Bank,* 6 November 2021) https://www.indusind.com/iblogs/pressrelease/clarification-on-news-article/

[7] Devgaon, 'Bharat Financial Inclusion rolls out Aadhaar-based instant cashless loan disbursal' (*The Hindu Business Line,* 22 February 2017) https://www.thehindubusinessline.com/money-and-banking/bharat-financial-begins-aadhaar-based-cashless-loan-disbursal/article64298830.ece

Objective of this report

Despite the increasing trend of consent scams by financial service providers, there has been very little regulatory action around the issue as even acknowledgement of the issue is seldom official. Even in the current instance, media reports suggest that the Reserve Bank of India, banking regulator that regulates the microfinance industry, was aware of the issues as early as September 2021, there has been no official statement from the banking regulator on the matter. Even in cases of active acknowledgement like the *Airtel Payments Bank Subsidy Scam,* while one provider was penalised and people got their money bank, the payment system which allowed the incident to happen and the payment system operator was not penalised and more importantly the underlying in remedying the system design problem of last Aadhaar linked account (LALA) getting the subsidy remained and is making subsidy payment diversions still possible, letting people run to get subsidy grievances redressed.

There is a need for extensive public documentation on the consent violations going to the root causes of system design issues instead of covering it up as a ***'Technical Glitch'*** and regulating system designs related to consent collection to prevent these consumer harms. This report aims to delve into the issue of **Bharat Financial Technical Glitch / Consent Scam** and investigate the claims to put facts around the incident, from open source intelligence (OSINT) analysis of publicly available information and document the findings for public record. The report also would like to make recommendations based on the findings to solve various issues surrounding Consent design, particularly in the context of digital lending.

2. Facts reported on BFIL 'Technical Glitch'

This section documents the chronology of events through available press reports on the matter.

WhistleBlower Claim

On November 5, 2021, *The Economic Times* reported[8] several people including senior employees of IndusInd Bank subsidiary, Bharat Financial Inclusion (BFIL) reported to Reserve Bank of India(RBI) and the board of bank highlighting lapses in governance and accounting norms to allegedly 'evergreen' loans running into thousands of crores since the outbreak of Covid-19.

S.No	Date	Sender	Letter	Sent to
1	September	Non-executive	Resignation letter citing - *"RBI*	Board of

[8] Sugata Ghosh, 'Whistleblowers raise loan evergreening issue at IndusInd arm (*The Economic Times,* 05 November 2021) https://economictimes.indiatimes.com/industry/banking/finance/banking/whistleblowers-raise-loan-evergreening-issue-at-indusind-arm/articleshow/87531018.cms

	15th, 2021	chairman of BFIL, M R Rao	*has raised issues with respect to BFIL particularly the 80,000 loans given in May 2021"*	IndusInd Bank
2	October 14, 2021	'Outside' whistleblower	suggestions to set up risk management and audit committees for BFIL were ignored, "process lapses" in extension of loan contracts, cash disbursement and accounting practices.	RBI
3	October 17, 2021 and October 24, 2021	'Internal' Whistleblowers	"adjusting new loan money with overdues from earlier loans", alleged transactions to dress-up the books	Some Independent directors of IndusInd Bank and RBI officials

Table 1: List of letters by multiple whistleblowers

It is evident from above that RBI was aware of certain issues pertaining to loans given in May 2021 as early as September 15th, 2021, yet has not acted to protect the consumer in any manner from publicly available information. As of Feb 2021, it still has not released a statement on the matter and has failed in protecting consumers.

IndusInd response, addendums

The IndusInd Bank responded to the whistle blower article through its press release[9] titled 'Clarification on news article' dated November 6, 2021 termed the anonymous whistleblower allegations as *'grossly inaccurate and baseless'.* While dismissing governance and control, evergreening issues, it added

- For pandemic induced stress to their client, they offered, "Additional loan with a longer tenor and lower EWI for customers, after they cleared their arrears and with their due consent."
- All the loans follow a weekly repayment model and the customers are required to make payments week on week; if there is any default, the same gets recorded as missed instalments. In view of the weekly repayment model, the concept of evergreening is infeasible.

Contradicting itself a few statements below, it also admitted to a 'technical glitch'

- Due to a technical glitch in May 2021, nearly 84,000 loans were disbursed without the customer's consent getting recorded at the time of loan disbursement. This issue was highlighted by the field staff within two days and the technical glitch was rectified

[9] (*IndusInd Bank*)

expeditiously. Out of the above, only 26,073 clients were active with the loan outstanding at Rs.34 crore, which is 0.12% of the September-end portfolio.

S.No	Date	Accounts	Outstanding
1	May, 2021	~84000	??
2	Nov 6, 2021	26073	₹ 34 Crore

Table 2: Users impacted, amount involved.

In a subsequent interaction with analyst Hemandra Hazari, IndusInd Bank clarified[10] that *"the loan disbursal systems are end-to-end digital in BFIL, without any manual intervention. In April, BFIL implemented a technology upgrade to its system. The biometric verification is sought for customer approval for the loan, and when it fails, a One Time Password (OTP) is sent to the customer's mobile, which is then inputted in the system for customer approval. However on May 21, 2021, on account of a bug in the system, the OTP stage got bypassed for those customers who could not record their biometrics, and the loans were disbursed."*

There was no mention if the 84000 people were notified about the 'Glitch', how the auto-consented loan was handled and what options / reasons consumers were given. In the absence of this information, one is forced to presume that everyone impacted by the glitch actually paid the price.

On December 3, 2021, *The Economic Times* reported that IndusInd bank has appointed Deloitte to review the whistleblower allegations.[11]

Corporate Politics and Market Movements

The whistleblower report led to a fall of over 10% on the stock of IndusInd Bank[12], causing $1.3 Billion loss to shareholder value. The publication of the whistleblower report was shortly after an announcement on November 3 by rival microfinance institution Spandhana Spoorthy hiring top management of BFIL.[13] This was followed by resignation of the Managing Director & CEO and the Executive Director & CFO which Bharat Financial notified the capital markets regulator in a filing and mentioned it is processing their release pending the external audit investigation into the whistleblower allegations.[14]

---

[10] Hemindra Hazari, 'IndusInd Bank Imbroglio: Evergreening or Just Plain Old Incompetence?' (*The Wire*, 11 November 2021) https://thewire.in/banking/indusind-bank-imbroglio-evergreening-or-just-plain-old-incompetence

[11] Mannu Arora, 'IndusInd Bank appoints Deloitte to review whistleblower allegations at arm Bharat Financial' (*ETCFO*, 03 December, 2021) https://cfo.economictimes.indiatimes.com/news/indusind-bank-appoints-deloitte-to-review-whistleblower-allegations-at-arm-bharat-financial/88074380

[12] George Mathew, 'Explained: Why IndusInd shares slid 10% on Monday' (*The Indian Express,* 09 November 2021) https://indianexpress.com/article/explained/indusind-bank-shares-loans-technical-glitch-7614496/

[13] Abhishek Kothari, 'Bharat Financial Inclusion'S Top Leadership Likely To Head To Spandana Sphoorty' (*CNBC,* 03 November 2021) https://www.cnbctv18.com/finance/bharat-financial-inclusions-top-management-likely-to-head-to-spandana-sphoorty-11334332.htm

[14] PTI, 'Bharat Financial Inclusion top officials resign to join rival Spandana Sphoorty' (*ETHRWorld,* 30 November 2021) https://hr.economictimes.indiatimes.com/news/industry/bharat-financial-inclusion-top-officials-resign-to-join-rival-spandana-sphoorty/88002528

This coupled with the fact of the resignation of MR Rao in September and RBI's knowledge of the matter before that, does indicate corporate politics at play besides the actual issue.

3. Scope of Investigation

Methodology

The scope of the investigation is to gather evidence from materials available publicly and study findings from the same to analyse / reconstruct the glitch as best as possible using open source intelligence (OSINT) techniques. Since we don't have access to any privy information, conclusions are impossible to arrive at. The intent there was to collate all publicly available information and attempt to visualise the jigsaw puzzle.

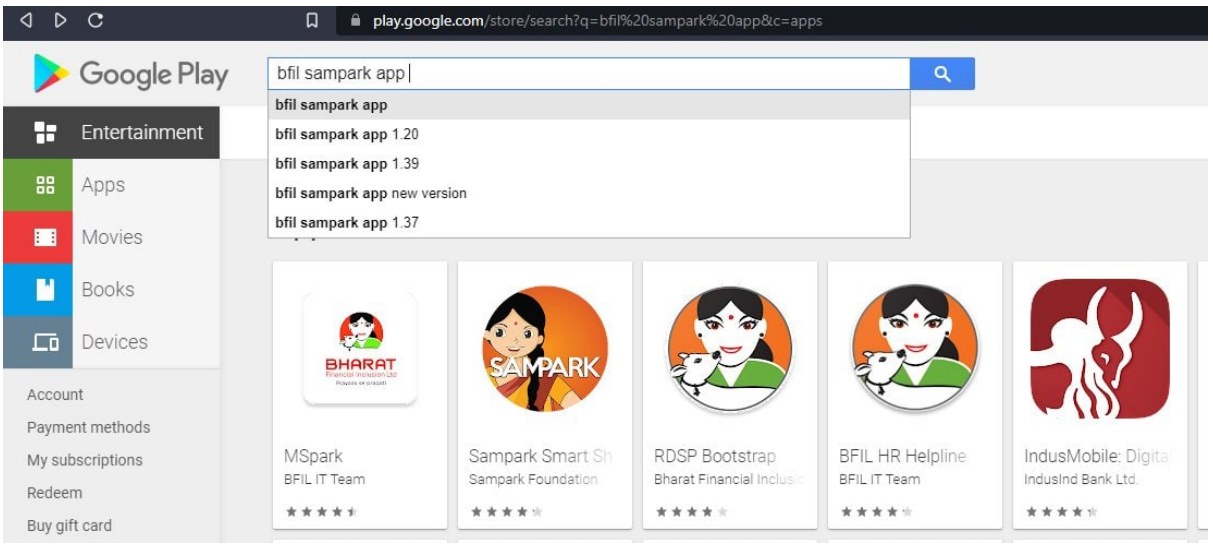
The data sources and mode of access to data is mentioned for each type of data. The procedure for analysis of app binaries involved analysing the apps with MobSF[15], an award winning automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. For the purpose of this investigation, static analysis was performed on all available binaries and source files were extracted from analysis and version controlled to see the difference between available versions of the app binaries

Data Sources

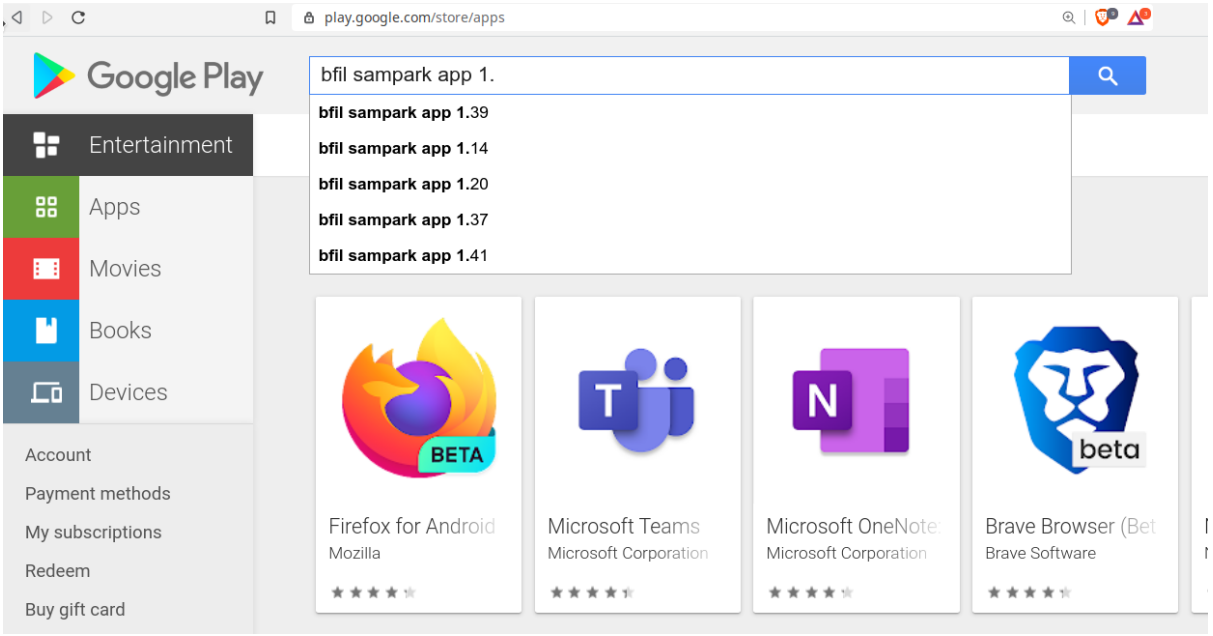
Google Play search suggestion data

One of the earliest steps in starting the investigation was to locate the app used by agents who service the borrowers. Searching for apps developed by 'BFIL' developer on Koodous[16] indicated that BFIL Sampark was the name of the app with package Id (com.bfil.member status)

[15] GitHub, Mobile-Security-Framework-MobSF
[16] Koodous, https://koodous.com/apks?search=developer:%27BFIL%27



- Searching for “bfil sampark app” on Google Play Store, returns a list of auto-suggest options that ought to have been populated by repeated search of those options by other users.



- Altering the search query to “bfil sampark app 1.” gave suggestions with specific version numbers, again indicating a large number of users had searched with such specific queries containing version numbers.
- The *BFIL Sampark app* - however seems to have been removed from Google Play since the incident / later date and is no longer publicly available.

Android apps

The following android binaries (apk files) of BFIL Sampark app (com.bfil.memberstatus) were sourced from Koodous[17]. Except for Version 1 that is signed with Google's certificate, others are signed with BFIL's certificate, so authenticity of the apk files can be reasonably ascertained to be original. The application binaries have been archived[18] from Koodous.

S.No	Version	SHA256 checksum	Koodous Upload Date	Env Type	Possible Date
1	1	b8971b613d864c6a93649a8a9220c63a3644b51c0ef55e2f85c975f44524a3be	Aug 19, 2020 2:51:52 PM	UAT	
2	1.14	b2c567aa88a10a69961c04807f27bab43e381df8eba7ffb43fe6a6bafd26e073	May 15, 2021 3:13:24 AM	UAT	
3	1.20	35cf04dda477c2281df4e5b3f9a8ee0f787da18f6f1126b35841d33e504f2035	May 15, 2021 3:12:16 AM	UAT	
4	1.28	ba1df8c81144a46925d236f888591872364aec27aa27ac844b041cd3f96083ba	Jul 20, 2021 8:41:01 PM	Prod	
5	1.38	adc4f05d309b707238936d8877ff6f19a61867a3ef5484e31ae2739513dde05e	May 15, 2021 3:16:44 AM	Prod	
6	1.41	a62cadc885cfaf7489152e73708613c6482d21e033efee6d8dec30993d84d35e	Jul 9, 2021 7:35:43 PM	Prod	

Table 3: List of various binaries of *BFIL Sampark* app along with version metadata

Aadhaar Authentication / eKYC Stats

UIDAI publishes daily statistics on authentication and eKYC on its dashboard.[19] In addition to overall ecosystem level statistics, they publish entity level cumulative statistics on the number of authentications performed via various authentication modes like fingerprint, demographic, OTP, and IRIS on a daily basis.

[17] Koodous, https://koodous.com/apks?search=com.bfil.memberstatus
[18] Filen, https://filen.io/f/e03ad74b-3b4d-4744-8ab9-f86c171aab2f#!7BTZ19TFCdXwiosFMjByfrOnLVw5BQ18
[19] Aadhaar Dashboard (*Unique Identification Authority of India*) https://uidai.gov.in/aadhaar_dashboard/

Aadhaar dashboard stats[20] is an archival tool that runs daily and archives a copy of published statistics. A script[21] was written to filter the data pertaining to Authenticating User Agency(AUA) / KYC User Agency(KUA) statistics of IndusInd Bank, parent entity of BFIL.

IndusInd Aadhaar AUA KUA Dashboard Statistics

id	eKYC	auth	FP	DM	IRIS	OTP	date	Delta eKYC	Delta auth	Delta FP	Delta DM	Delta IRIS	Delta OTP	Delta Date
1308358087	37280910	164433547	128695602	30390402	2130721	2571400	2021-06-01	15988	149938	131336	13059	11	4329	1
1305666142	37264922	164283609	128564266	30377343	2130710	2567071	2021-05-31	7461	72644	65557	3875	0	3196	1
1304235120	37257461	164210965	128498709	30373468	2130710	2563875	2021-05-30	17377	164361	144170	14230	12	5006	1
1303454095	37240084	164046604	128354539	30359238	2130698	2558869	2021-05-29	32950	330524	284308	33601	27	10361	1
1301330147	37207134	163716080	128070231	30325637	2130671	2548508	2021-05-28	0	0	0	0	0	0	1
1297949260	37207134	163716080	128070231	30325637	2130671	2548508	2021-05-27	16603	161153	148135	7303	10	5007	1
1294372565	37190531	163554927	127922096	30318334	2130661	2543501	2021-05-26	20570	232037	210439	13952	8	5142	1
1291004265	37169961	163322890	127711657	30304382	2130653	2538359	2021-05-25	29922	306746	282724	10669	35	8735	2
1286718455	37140039	163016144	127428933	30293713	2130618	2529624	2021-05-23	16432	221901	204083	11688	0	4413	1
1284973101	37123607	162794243	127224850	30282025	2130618	2525211	2021-05-22	17915	300299	256486	26368	62	11309	1
1282459497	37105692	162493944	126968364	30255657	2130556	2513902	2021-05-21	16557	0	0	0	0	0	1
1279042413	37089135	162493944	126968364	30255657	2130556	2513902	2021-05-20	18905	164464	142478	13893	3	6147	1
1275600646	37070230	162329480	126825886	30241764	2130553	2507755	2021-05-19	18945	314012	265736	26802	7	12543	1
1270428079	37051285	162015468	126560150	30214962	2130546	2495212	2021-05-18	13766	0	0	0	0	0	1
1267183730	37037519	162015468	126560150	30214962	2130546	2495212	2021-05-17	5473	75900	70336	2446	0	3107	1
1265445552	37032046	161939568	126489814	30212516	2130546	2492105	2021-05-16	12239	103184	90073	7269	13	5722	1
1264478770	37019807	161836384	126399741	30205247	2130533	2486383	2021-05-15	11193	115981	100274	11158	58	4110	1
1262301161	37008614	161720403	126299467	30194089	2130475	2482273	2021-05-14	15162	128731	111287	11622	64	5191	1
1259539768	36993452	161591672	126188180	30182467	2130411	2477082	2021-05-13	14896	293434	253039	27834	22	11563	1
1255789421	36978556	161298238	125935141	30154633	2130389	2465519	2021-05-12	14895	131441	116482	9057	15	5618	1
1252428262	36963661	161166797	125818659	30145576	2130374	2459901	2021-05-11	14010	0	0	0	0	0	1
1249188369	36949651	161166797	125818659	30145576	2130374	2459901	2021-05-10	3303	48577	44836	1658	0	2073	1
1247800768	36946348	161118220	125773823	30143918	2130374	2457828	2021-05-09	6565	78803	62883	11565	1	4025	1
1246945857	36939783	161039417	125710940	30132353	2130373	2453803	2021-05-08	32432	302011	252084	38214	55	10668	2
1240719702	36907351	160737406	125458856	30094139	2130318	2443135	2021-05-06	59774	532511	470421	42060	61	17945	4
1229702962	36847577	160204895	124988435	30052079	2130257	2425190	2021-05-02	6905	75211	63312	8266	2	3408	1
1228634976	36840672	160129684	124925123	30043813	2130255	2421782	2021-05-01	19309	206695	183679	16733	4	3592	1
1226105968	36821363	159922989	124741444	30027080	2130251	2418190	2021-04-30	49815	393535	347990	35745	36	7982	2

Table 4 : IndusInd Aadhaar AUA KUA Dashboard Statistics for the month of May 2021 [22] (id - Job ID collecting the data, eKYC - cumulative number of eKYC requests, auth - cumulative number of authentication requests, FP - Fingerprint authentication, DM - demographic authentication, IRIS - Iris authentication, OTP - OTP authentication)

BFIL Agent data

Bharat Financial has publicly put out COVID passes[23] for their agents to commute during lockdown situations. This indicates, a total of ~19300 agents were involved in servicing activities across the country in April 2020. A map / hourly graph of all the 84000 consent-less loans and their geographic / temporal spread can provide a hint if there were specific concentrations in any region / any set of agents to indicate if the said loans were indeed part of 'Glitch' / any coordinated malpractice. Since we don't have access to specific information on this, we cannot make use of this data in any meaningful way, but the auditors having access can add confidence to their finding corroborating this data.

[20] Srikanth Lakshmanan, Aadhaar dashboard stats (*GitLab*) https://gitlab.com/srikanthlogic/aadhaar-dashboard-stats
[21] GitLab, Get Single KUA AUA Stat
[22] IndusInd Authentication eKYC Statistics, https://docs.google.com/spreadsheets/d/1GSWRK4fTpdea_jxpt90fq5-hLXDEgo0xvWMxUWbrXGc/edit?usp=sharing
[23] AuthorizationLetter, https://bmsapi.bfil.co.in/AuthorizationLetter/

Findings

Date of incident, Version of app

1. The analyst's call with Hemindra Hazari, as reported, tells of the incident ‘technical glitch’ that happened on May 21, 2021. The same analyst also noted the ‘technical glitch’ was highlighted in 2 days and *rectified* without giving a timeline. It is hence safe to assume the ‘glitch’ lasted for several days.
2. Production build of BFIL Sampark app v1.38 was uploaded to Koodous on May 15, 2021.
3. The presence of search terms *bfil sampark app 1.37* and *bfil sampark app 1.39*, besides *bfil sampark app 1.41* in Google Play auto suggest data for ***bfil sampark app 1.***
4. Both the above make v1.38 and 1.41 of special interest in analysing.

Aadhaar authentication / eKYC statistics

1. Although available most days in the month, the data is unreliable to come to conclusions for 2 reasons.
    a. Unreliability of Aadhaar dashboard - as multiple days (Including May 21 incident day) have 0 authentication transactions. It gets even more complicated with it showing eKYC transactions on days with 0 authentication transactions. This was cross-verified for multiple AUA / KUA and is a generic problem in data updates in the dashboard.
    b. While the IndusInd admission itself agreed that biometric authentication was not used and the glitch was in OTP, analysis of the apps reveal, the OTP authentication for many scenarios in the agent app was using a MFI run OTP service and not Aadhaar OTP authentication. Further for renewal of loans, eKYC was not performed as they are already existing customers of MFI.
2. The UIDAI numbers are for IndusInd bank and there could be use of Aadhaar infrastructure outside of BFIL Sampark app by other services of banks. Having said these, the sharp dip on several days in eKYC numbers, coupled with 0 authentication transactions are a cause for concern and needs to be probed.

Technical Analysis of Android App and Reversed Source Code

1. Sahayata Loan is a special type of loan offered by BFIL to help people get additional credit, after offsetting the past dues with this loan. If there was a consent bypass, agents can use evergreen (process of issuing fresh loans to outstanding accounts for settling the dues to show the loans were repaid and are not non-performing assets) - unserviceable accounts without the knowledge of the customer.
2. Sahayata Loan was first seen in V1.28 among the versions of apps we have access to. Sahayata Loans are 0 disbursement loans, meaning they only offset past dues and do not disburse any amount to the borrower.
3. In the versions analysed, consent for Sahayata loans is only OTP based and biometric consent is needed only if there is a disbursement. Unlike an Aadhaar

authenticated biometric consent where a transaction is recorded on the UIDAI side, the OTP consent is against an OTP server run by BFIL that sends a 4 digit OTP.

4. The URLs of Dynamic URL service (Table 5), which load on the app Home screen pulling various server URLs the app needs to communicate to. One can see its changed version in v1.38 and v1.41. But since the backend code is not available for access, we cannot ascertain if that change was due to a bug / oversight (deployment pointing to a lower version of the service) / malpractice.
5. Further, a difference between v1.38 and v 1.41 does not indicate major differences in client side flow, particularly to OTP, hence it is most likely a service side change that fixed the issue after 2 days.
6. The client-side app on the analysed versions does not have special bugs to skip entering OTP, so in all likelihood, an OTP was entered for all the 84000 loans and the glitch could be in validation. This gives room for the malpractice theory, but we cannot ascertain the same using available data. There are 2 possibilities on how the malpractice could have happened and the validity of both can be ascertained by logs of SMS sent to the customer. This should be available with the telco partner of BFIL as part of their system of storing SMS metadata for the TRAI anti-spam blockchain for combating spam.
    a. No OTP was sent to customers and any 4 digit entered by the agent was validated as OTP and agents were instructed to ‘evergreen’ these 84000 accounts. In this case, a forensic audit of the server hosting BFILAggregatedService with deployment logs can help to identify if a buggy code was patched and later replaced by a patch to fix the ‘glitch’.
    b. The OTP validation was not tampered, but instead the customer database was tampered to have the mobile number of agents for these 84000 accounts, so that when the agents evergreen, they instead of customers get the OTP and can key in to create a new loan account, without the knowledge of the customer. In this case, the ‘glitch’ could be easily fixed without a code fix as updating the database back to the customer's original number is all that is needed.
7. The apps also indicate that the development process included UAT and Production as can be seen in builds of the app binaries. If this is true, it is glaring that a serious bug as this was not caught in UAT.

S.No	Version	Dynamic URL Service
1	1.0	https://103.231.212.182:8443/BFILAggregatedService-v1.51_DynamicURL/PBAggregatedServices/
1	1.20	https://103.231.212.182:8443/BFILAggregatedService-v1.51_DynamicURL/PBAggregatedServices/
2	1.28	https://103.231.212.182:8443/BFILAggregatedService-v1.51_DynamicURL/PBAggregatedServices/
3	1.38	https://AepsAgs.bfil.co.in:8443/BFILAggregatedService-v1.25_DyamicURL/PBAggregatedServices/
4	1.41	https://AepsAgs.bfil.co.in:8443/BFILAggregatedService-v1.25

		_DyamicURL/PBAggregatedServices/

Table 5 :- List of backend URLs various versions of app communicate to for loading configuration data

Limitations

S.No	Data Source	Information	Analysis	Notes
1.	Koodous	App Name, App binaries	Narrowing down the app, multiple versions of the app.	Partially conclusive
2	Aadhaar Dashboard	Authentication / eKYC Statistics	UID authentication activity in incident month	Inconclusive, unused for Sahayata.
3	Google Play search suggestion data	App Versions	Narrowing down the version of the app.	Inconclusive
4	MobSF - Technical analysis	Technical analysis of apps	Inspect the reversed binaries for consent bypass, understand execution flow.	Partially conclusive.
5	BFIL Agent data	Geographical spread	Incomplete.	Corroborative value.

Table 6 :- Limitations of analysis of various data sources

Summary

1. The available public evidence suggests some specific areas to be investigated. Citizens' report will wait for the external auditors official report.
2. The evidence available in public is insufficient to arrive at a conclusion, but the entire episode has thrown up an important oversight issue in relation to consumer consent in digital lending.
3. Transparency, Notice are key expectations from regulator, auditors to strengthen consumer protection and increase trust.

4. Recommendations

1. Publish Standard Operating Procedure (SOP) for banking regulators to handle whistleblower complaints when consumers are affected with due notice, redress options. Regulatory silence on unfair conduct reportage affects consumers, silence reporters. (To RBI)

2. Extend publication of application checksums referred in DPSC directions to banking apps used by consumers, as well as agents. (To RBI)
3. Publish the external audit report publicly (To IndusInd board, RBI, SEBI), detailing forensic evidence, methodology to verify the assertions being made. Create a repository of all such reports where incidents of consumer harm have happened to serve as an archive of historical incidents and regulatory responses.
4. Publish the action taken, especially in reversing / addressing the consumer harm caused by the unfair conduct. (To RBI)
5. Publish UIDAI Authentication, eKYC dashboard data (A high frequency indicator) in a consistent way, in machine readable format to detect anomalies in consent practices. (To UIDAI)
6. Analyse OTP abuse and revisit the role of OTP in consent. (Government, Industry, Regulators, Consumers)
7. Fast-tracking investigations, especially in case of UIDAI, as logs are retained only for 6 months and only the AUA retains logs for longer durations. In case of banks, since they themselves are AUAs, attempts are proving that Aadhaar malpractice is becoming harder as time passes. (To UIDAI, LEA)

5. References

1. Grameen Foundation. “Full Financial Inclusion in India? How the 'JAM Trinity' Can Help Businesses Make it a Reality.” *NextBillion*, 18 July 2017, https://nextbillion.net/full-financial-inclusion-in-india-how-the-jam-trinity-can-help-businesses-make-it-a-reality/ Accessed 12 February 2022.
2. Venkatanarayanan, Anand. “Aadhaar Mess: How Airtel Pulled Off Its Rs 190 Crore Magic Trick.” *The Wire*, 21 December 2017, https://thewire.in/banking/airtel-aadhaar-uidai Accessed 12 February 2022.
3. Julka, Harsimran. “The dangers of instant Aadhaar authentication for India's 1-minute loan market.” *Moneycontrol*, 1 March 2018, https://www.moneycontrol.com/news/business/startup/the-dangers-of-instant-aadhaar-authentication-for-indias-1-minute-loan-market-2519013.html Accessed 12 February 2022.
4. Banerji, Olina, et al. “The making of a loan crisis at Byju's.” *The Ken*, 27 May 2019, https://the-ken.com/story/the-loan-crisis-at-byjus/ Accessed 12 February 2022.
5. Kauntia, Nishant, et al. “Byju's predatory practises flagged in Parliament by MP Chidambaram.” *MediaNama*, 14 December 2021, https://www.medianama.com/2021/12/223-byjus-loan-sharks-mp-chidambaram/ Accessed 12 February 2022.
6. IndusInd Bank. “Clarification on news article.” *IndusInd Bank Press Releases*, IndusInd Bank, 6 November 2021, https://www.indusind.com/iblogs/pressrelease/clarification-on-news-article/ Accessed 12 February 2022.
7. Devgaon. “Bharat Financial Inclusion rolls out Aadhaar-based instant cashless loan disbursal.” The Hindu Business Line, 22 February 2017, https://www.thehindubusinessline.com/money-and-banking/bharat-financial-begins-a

adhaar-based-cashless-loan-disbursal/article64298830.ece Accessed 12 February 2022.
8. Ghosh, Sugata. “Whistleblowers raise loan evergreening issue at IndusInd arm.” The Economic Times, 5 November 2021, https://economictimes.indiatimes.com/industry/banking/finance/banking/whistleblowers-raise-loan-evergreening-issue-at-indusind-arm/articleshow/87531018.cms Accessed 12 February 2022.
9. (IndusInd Bank)
10. Hazari, Hemindra. “IndusInd Bank Imbroglio: Evergreening or Just Plain Old Incompetence?” *The Wire*, 11 November 2021, https://thewire.in/banking/indusind-bank-imbroglio-evergreening-or-just-plain-old-incompetence Accessed 12 February 2022.
11. Arora, Mannu. “IndusInd Bank appoints Deloitte to review whistleblower allegations at arm Bharat Financial” *ET CFO*, 3 December 2021, https://cfo.economictimes.indiatimes.com/news/indusind-bank-appoints-deloitte-to-review-whistleblower-allegations-at-arm-bharat-financial/88074380 . Accessed 12 February 2022.
12. Mathew, George. “Explained: Why IndusInd shares slid 10% on Monday | Explained News.” *The Indian Express*, 9 November 2021, https://indianexpress.com/article/explained/indusind-bank-shares-loans-technical-glitch-7614496/ Accessed 12 February 2022.
13. Kothari, Abhishek. “Bharat Financial Inclusion'S Top Leadership Likely To Head To Spandana Sphoorty.” *CNBC TV18*, 3 November 2021, https://www.cnbctv18.com/finance/bharat-financial-inclusions-top-management-likely-to-head-to-spandana-sphoorty-11334332.htm Accessed 12 February 2022.
14. PTI. “Bharat Financial Inclusion top officials resign to join rival Spandana Sphoorty.” *ETHRWorld*, 30 November 2021, https://hr.economictimes.indiatimes.com/news/industry/bharat-financial-inclusion-top-officials-resign-to-join-rival-spandana-sphoorty/88002528 Accessed 12 February 2022.
15. https://github.com/MobSF/Mobile-Security-Framework-MobSF/
16. https://koodous.com/apks?search=developer:%27BFIL%27
17. https://koodous.com/apks?search=com.bfil.memberstatus
18. https://filen.io/f/e03ad74b-3b4d-4744-8ab9-f86c171aab2f#!7BTZ19TFCdXwiosFMjByfrOnLVw5BQ18
19. Unique Identification Authority of India. “Aadhaar Dashboard.” *UIDAI*, https://uidai.gov.in/aadhaar_dashboard/ Accessed 12 February 2022.
20. Lakshmanan, Srikanth. “Srikanth L / aadhaar-dashboard-stats · GitLab.” *GitLab*, https://gitlab.com/srikanthlogic/aadhaar-dashboard-stats Accessed 12 February 2022.
21. https://gitlab.com/srikanthlogic/aadhaar-dashboard-stats/-/snippets/2247068
22. IndusInd Authentication eKYC Statistics
23. https://bmsapi.bfil.co.in/AuthorizationLetter/

6. About

Versions

S.No	Version	Date	Comments
1	Draft - 0.1	12 Feb 2022	Initial draft
2	0.2	14 Feb 2022	Updated with OTP hijack possibility.
3	1	15 Mar 2022	Review feedback comments.

Credits

- Anish TP, Hasgeek - ArtWork
- CaptNemo, CashlessConsumer - Source Controlling reverse code for analysis.
- Srikanth L, CashlessConsumer - Authoring Report
- Rohin Garg & Tejasi Panjiar, Internet Freedom - Review, Explainer

Digital Lending WatchTower

DigitalLending WatchTower aims to keep track of the digital lending space in India and have ongoing conversations about digital lending primarily from the lens of consumer protection.

CashlessConsumer

CashlessConsumer is a consumer collective working on digital payments to increase awareness, understand technology, produce / consume data, represent consumers in policy of digital payments ecosystem to voice consumer perspectives, concerns with a goal of moving towards a fair cashless society.