TRAINING TOOL ON DATA PRIVACY:
CLIENT PROTECTION

Lead Author: Amit Gupta

December 2014

Keeping clients first
in microfinance

This training tool is based on the 6 Client Protection Principles of the Smart Campaign and focuses on data privacy practices for financial service providers. Please note that this framework is outdated**,** as the sector now follows 8 Client Protection Standards**.** The document uses real-life case studies to highlight common data privacy risks and errors, while providing guidance for staff training and client education.

Key words: Data Privacy in Microfinance - Training Tool on Data Privacy - Financial Service Providers India - Client Data Protection Case Studies - CPP Training Tool - Microfinance Client Rights

Training Tool on Data Privacy

Client Protection Principle

Note: It is important to note that the original 6 Client Protection Principles have now evolved into 8 Client Protection Standards.

The Smart Campaign's Client Protection Principle 6, Privacy of Client Data, states that,

"Financial service providers (FSPs) should respect client data in accordance with the laws and regulations of individual jurisdictions, and should only use data for the purposes specified at the time the information is collected or as permitted by law, unless otherwise agreed with the client".

In simple terms, the principle affirms that clients share very important personal and financial information with FSPs and that it is the responsibility of FSPs to protect the privacy and confidentiality of such data. If a FSP has to share the client data with outside agencies, it should seek necessary approval from the client before sharing the data.

Background

Data privacy is often neglected by many Indian FSPs. Experiences from detailed client protection assessments and interactions with FSPs during CPP trainings show that FSPs have scored lowest on the Data Privacy principle (2.4 out of 5 based on client protection assessments; more than 70 percent assessed institutions have scored less than adequate on the principle). In general, FSPs have inadequate policies and practices around this principle. Most of the time, institutions do not quite understand the relevance of the principle and also do not know how to train staff or clients in order to ensure client data privacy.

Objective of the Tool

The current tool illustrates what could go wrong if proper policies and procedures are not followed. In the above context, this tool can be used by FSPs:

1. As part of their training materials to instruct staff on the importance of maintaining data privacy.
2. In order to further adapt the case studies to educate their clients.

Each of the case studies presented in this tool are based on the experiences of actual Indian FSPs, who have suffered from weaknesses in their data privacy practices or have faced real threats due to privacy concerns. Though the names of the FSPs and clients are fictional, the case studies highlight real issues.

Case Studies

There are case studies presented in this tool. The examples focus on (i) lack of written data privacy policy and its active communication with clients; (ii) client's identity theft for procuring unsolicited advantages like state offered subsidies or purchase of mobile SIM cards; (iii) staff committing fraud by creating ghost clients based on Know Your Customer (KYC) documents. The case studies also discuss (iv) misrepresentation of client information to seek institutional benefits in the form of soft funds and (v) unauthorized use of client personal information and photos in marketing and communication purposes.

Table of Contents

Case Study 1: Importance of receiving written consent for use of client photos and information in public documents and marketing materials

Relevant indicators

Standard	Indicators
6.2 The FSP informs clients about when and how their data is shared and gets their consent	**6.2.4** The FSP informs customers how their information will be used internally and, when applicable, when it will be shared externally.
	6.2.8 The FSP requires written client consent to use of information or photos in promotions, marketing material and other public information.

Personal information should not be made public unless the client understands how the information will be used, and provides consent. This case study demonstrates how failure to obtain written consent can damage the relationship between the client and the institution.

Parivartan and its unauthorized communication

Parivartan is a well-established FSP in southern India that regularly publishes client "success stories"—short profiles of clients who have used financial services to improve their lives. One such profile told the story of a client named Shubham, a restaurant owner in his third loan cycle. Mr. Shubham had used his loans to purchase a number of productive assets including a mixer-grinder, juicer, and cooking range. As a result, the business had improved significantly, and the client was being recruited by several other FSPs who offered larger loan sizes.

Parivartan wanted to showcase Mr. Shubham's success story and therefore took some pictures of the client and his restaurant, and published these in their product brochure, annual report, and on their website. The FSP did not seek the client's verbal or written approval before using his picture for promoting the institution, but this did not bother Mr. Shubham, who proudly displayed the materials in his restaurant.

One day many months later, one of Mr. Shubham's regular customers—a lawyer—visited the restaurant. Seeing the promotional materials, he casually inquired about whether Parivartan had compensated Mr. Shubham for his role in promoting the FSP. Mr. Shubham replied that not only had he not received any payment, but he had been surprised to see his picture on the materials. He had not been consulted and had assumed that the photos taken by his loan officer were strictly for the purposes of the loan application. The lawyer was shocked to hear Mr. Shubham's story and sensed an opportunity to sue Parivartan on the basis that the FSP had used the photos for commercial gains without any written communication and consent.

Though Mr. Shubham did not go through with the lawsuit, he did confront his loan officer about why he had not been consulted and compensated. The loan officer raised the issue with his branch manager, who escalated the issue to senior managers.

Management soon realized that they had narrowly escaped a costly legal battle and decided to create a policy on obtaining client consent before using client photos in any public format. They added a simple

policy to the Parivartan credit manual and supplied loan officers with a client consent form. Loan officers also received training on how to communicate with clients about the use of their photos, and to use the consent form.

Application for other institutions

Many FSPs take pictures of clients and publish them in various promotional or communications materials such as brochures, case studies, annual reports, and impact studies. However, very few of these institutions regularly explain to clients how their photo will be used and seek client consent. Clients have the right to know how their image will be used and to decide whether they accept this or not. To strengthen practice in this area, FSPs should implement a policy that requires relevant employees (e.g., field officers) to explain to clients how their photos will be used and to obtain their written consent. FSPs should also provide employees with a standard consent form and explain how they should use it with clients.

Case Study 2: Importance of establishing policies for privacy of client information, appropriate use of KYC documents, and penalties for staff for misuse of client identity documents.

Relevant indicators

Standard	Indicators
6.1 The FSP has a privacy policy and appropriate technology systems	**6.1.1** The FSP has a written privacy policy that governs the gathering, processing, use, distribution and storage of client information. The policy covers current staff and those who leave the organization and information leakage.
	6.1.3 The FSP's Staff Book of Rules and/or Code of Conduct penalize misuse or misappropriation of client data.
	6.1.4 The FSP has penalties for exposing or revealing client data to third parties without prior client consent.

The below case study describes how in the absence of properly educating new staff on the data privacy policy and setting examples of staff penalized on account of information misuse, a FSP suffered heavy financial losses.

Ashok Rai and his accomplice

Ashok Rai joined Sanket FSP as a Branch Manager after a long stint with a leading private bank in Maharashtra. Sanket and the Private Bank work with the same set of clients. From his previous job, Ashok has photocopies of 60 clients indentify proof documents like - election card, ration card, pan card, driving license. Since Ashok lives in the same area, he also has the information of all the clients and their households including their occupation, age, assets, livelihoods etc.

In his new role as a branch manager at Sanket, Ashok soon realized the critical role of Know Your Customer "KYC" documents in the credit approval process. Ashok colluded with the loan officer and used the photocopies of KYC documents and other client related information to create two ghost centers of about 30 and 20 clients each.

As per the FSP process, the loan officer formed the group and conducted compulsory group training, the branch manager (Ashok) approved the group (in group recognition test), and loans were issued of Rs. 8,000 to Rs. 15,000 to 50 clients from Sanket FI. Within a week of disbursement (which was fake) both Ashok Rai and the loan officer went on long leave under the guise of mother's illness and father's death, but never returned to Sanket FI.

Application for other institutions

Ghost clients created based on KYC documents have resulted in severe financial losses to FSPs. To prevent this, FSPs should have a clear policy governing the gathering, processing, use, distribution and storage of client information. As new staff members join the organization, FSPs need to ensure that all staff is trained on the data privacy policy and required to sign a document stating they have understood the policy and will abide by it. FSPs should also establish upfront penalties and punishments for breaching the privacy policies; it is critical for the FSP to share during induction and refresher trainings examples of staff who have broken the policy leading to fraud and the punishment given to offenders (i.e. termination of employment, in case of financial fraud – recoveries made, or fraudulent staff handed over to police etc to set a clear example for the rest of employees).

Case Study 3: Importance of training group leaders to safeguard member information and ensure that members regularly check account information

Relevant indicators

Standard	Indicators
6.2 The FSP informs clients about when and how their data is shared and gets their consent	**6.2.9 [group lending]** The FSP trains group leaders to safeguard group member information, particularly saving account balances, dates of loan disbursement, and information on repayment problems.

Group leaders have access to sensitive information about other clients and should be held to high standards of responsibility. Also from a transparency perspective, Smart Campaign clearly states that the FSP regularly gives clients clear and accurate information regarding their accounts (e.g., account statements, receipts, balance inquiries, proof of payment for loans; 3.5.3). It is therefore critical that FSPs provide up to date account information and each member regularly checks their account status.

Sharda Devi Center

Sharda Devi Center, a grameen-style center, was founded in Gorakhpur five years ago and now has 20 members. A well-respected woman named Shakuntala Bai has been the Center Leader for last three years and has gained the trust of other group members. In her capacity as the Center Leader Ms. Shakuntala helps other members to mobilize their KYC documents and fill the application forms. She also collects repayments from members and deposits the money with the FSP in weekly Center meetings.

After three years without experiencing any trouble, the loan officer assigned to the Sharda Devi Center noticed that group members were missing group meetings, and several were late on their payments. The loan officer visited the delinquent clients to understand what had gone wrong. The first client was surprised to discover that she was considered delinquent. She recounted to the loan officer how she had given her payment to Shakuntala a week prior, with the understanding the repayment would be made during the next group meeting. The client was not able to attend the meeting herself, as her child was ill, but she trusted that Shakuntala would make the payment on her behalf.

A second client had a similar story. The loan officer inquired as to whether the client checks her passbook to verify that Shakuntala had delivered the payment. The client responded that Shakuntala insisted on keeping their passbooks in her own possession, and did not offer to let them see whether the passbooks had been updated after meetings. The third client visited by the loan officer had a different story; Shakuntala Devi is friends with her elder sister and told her friend about the loan disbursed to the client. After the loan was received by the client, her elder sister came and took the money from the client, allegedly for health reasons. Now the client is under stress as she does not have sufficient money to make regular weekly repayments. The loan officer realized that Shakuntala Devi was exploiting her position in the group and that if urgent action was not taken quickly, her actions would have led to even more severe fraud.

Application for other institutions

Group leaders hold positions of authority and are entrusted with very sensitive information about other members. Many FSPs rely extensively on the center and group leaders as a conduit between the FSP and other member clients. Too often Center Leaders have exploited this situation to their advantage as discussed in the above case study. To make sure such instances do not happen, it is vital for FSPs to train members and group leaders on the importance of keeping member passbooks safe and private, and warning all members to not leave their passbook with anyone, including the group and center leader.

Members should also be educated as to how to check if their credit officer is updating the passbook regularly and if their account balances are in order (i.e. passbooks record the correct number of repayments made, amounts re-paid, and outstanding balance). Center Leaders should be specifically educated not to share savings and disbursement details with anyone outside the group. Regular operational monitoring and internal audits should also keep a strong check on whether or not members are retaining and carrying their passbooks with them at the end of center meeting. Active grievance redressal mechanisms can also provide clients with an opportunity to express their concerns and problems.

Case Study 4: Importance of informing customers how their information will be used internally, and when applicable, share externally

Relevant indicators

Standard	Indicators
6.2 The FSP informs clients about when and how their data is shared and gets their consent	**6.2.4** The FSP informs customers how their information will be used internally and, when applicable, when it will be shared externally.

FSIs, especially donor driven institutions (i.e. institutions dependent on soft funds), often present client stories in order to make potential donors more sympathetic to their work. In order to effectively provoke emotions, clients facts, figures, stories and photographs are often manipulated by FSIs without the consent of clients; clients are misrepresented, shown as being extremely destitute and completely dependent on donor generosity to survive. The case study below describes a similar situation where a FSP manipulates a client's information, story, and pictures to receive funds from donor; however, the aggrieved client is hurt by the FSP behavior and intends to stop his relationship with FSP.

Rahmatullah's story

Rahmatullah received a loan last year from Shubham, an NGO-MFI, and he is towards the end of his loan cycle, having repaid his installment regularly without fail. Last month, Shubham staff members approached him suggesting they wanted to conduct a photo shoot of him and his family, as well as get some personal and family details because Shubham is approaching some donors in western countries. The staff members said the donors are looking to provide funds to people like Rahmatullah so they can improve their quality of life.

During the photo shoot Rahmatullah was bit skeptical, as the photographer kept focusing on aspects which Rahmatullah and his family were trying to cover up, such as broken and dirty utensils, unkempt walls, etc. The photographer also took pictures of his children when they wore their old and worn out clothes, instead of new clothes Rahmatullah had bought for them. Since that day, Rahmatullah was anxious and unclear about the outcome of photo shoot and why the photos and information about his family were collected in the first place. However, a couple of days ago a Shubham loan officer approached Rahmatullah and said his new loan has been approved, because the NGO had received funds from abroad, and that he should come to the branch to collect his loan.

When Rahmatullah reached the branch to receive his new loan, he also asked about the photos and story shown to the foreign donors. The branch manager read the details of the published story to him, and showed him the pictures posted on website; the essence of the story was that Rahmatullah was an impoverished man. The story implied that some days he and his family go without food, that he has no stable source of income and that without money from the donor, he and his family will never escape poverty! Rahmatullah felt insulted and frustrated with the way his story was presented, as none of it was true. Sure, Rahmatullah is not a wealthy man, but he is also not so poor that his family goes hungry; he has worked very hard over the years to ensure that he can make ends meet. Rahmatullah has only taken a loan to improve his business, and he has been a regular payer. Because of this misleading

portrayal of him and his family, Rahmatullah seeks to end his relationship with the FSP and demands that the story be removed from the website immediately.

Application for other institutions

FSPs have a fiduciary responsibility to protect the confidentiality, security, accuracy and integrity of customers' personal and financial information. In the above example, the FSP breached the client's trust by showing him and his circumstances in negative light in order to elicit sympathy from donors, instead of showing the client as a hard-working person who needs financial support to strengthen his enterprise and continue supporting his family. In order to prevent this, it is the FSP's responsibility to cross-check with each client whether he or she is satisfied and comfortable with the way his or her story is published by the institution. A written client consent form should be signed by the client to demonstrate his or her agreement with what the FSP want to publish. In the case of a minor used in communications materials, written permission should be obtained from a parent or guardian.

Case Study 5: Importance of safeguarding physical files at branches and regional offices

Relevant indicators

Standard	Indicators
6.1 The FSP has a privacy policy and appropriate technology systems	**6.1.7** If files are stored in physical format, the FSP stores the client files in a secure location, within the branch or headquarters that has 1) restricted access only to selected persons; 2) is kept in a facility secure from arson or theft.

The case study below describes a situation where a FSP is facing criticism about identify theft of its clients and data being misused in variety of ways. The reason for identity theft can be traced to clients' physical files lying out in the open at a branch.

Chetana – Case of Missing Files

In the last two weeks, Orissa-based MFI Chetana has received about 16 complaints from three branches in the Bhuvneshwar district, where clients have accused the FSP of using their identity documents such as their PAN Card, Aadhar number (unique identity card), and Voter ID card to purchase mobile SIM cards, authorized quotas of gas cylinders and associated subsidies. From a security perspective, with the severe Naxalite movement in the state, Chetana's management is aware of the grave consequences for unauthorized purchases of SIM cards under their clients' names (or their family members' names) and their subsequent use by Naxalites. Management is also aware that the shopkeepers selling the SIM cards are only concerned with getting a photocopy of the required identity document and do not really check if the person buying the SIM card is the same as the one pictured in the identity document.

Misappropriation of gas cylinders on the subsidy given by the government to the client is both a financial and entitlement loss of client. (The government provides a limited number of subsidized cylinders to low income households to meet their annual needs, and black marketers are on the lookout for ways to procure these cylinders at a low cost and sell them at commercial rate.)

Chetana's management set up a committee to identify the reasons for this information theft; the committee visited the relevant branches to look through the files of aggrieved clients, and indeed in some of the files the identity documents were missing and in other cases the client files were missing altogether. The investigation committee noticed that all the clients files were lying out in the open in the central hall, where there are often many clients during disbursement (in general there is quite a bit of commotion during disbursement) and where clients or their family members go in order to make repayments to branch. The committee also observed that it is very easy for branch staff members to take any document from the files, or take the entire file, as staff stay in the branches and have 24-7 unrestricted access to the files.

Application for other institutions

The above example is a common observation amongst FSPs that keep client files out in the open where large numbers of clients or their family members visit to collect loans or make repayments. It is also common when the FSP's staff (BM and LOs) stay at the branch and have an unrestricted access to all the client documents and files. To prevent identity theft from physical files the FSP should make sure all the client files are stored in a separate room or a location away from the easy access of staff members or other visitors to the branch. Client files can also be stored in a locked cupboard *(Almirah)* to protect them from the internal staff residing at the branch. On a regular basis, the operations and internal audit department should also keep a vigil watch on how files are maintained, stored, and secured in the branch: whether the branch staff is maintaining password privacy, if they have access to computers for data entry, etc. On a regular basis, client files must be shifted to regional offices or headquarters in order to ensure proper management of files at branch level.