August 2014

FINCA Azerbaijan: *Protecting client privacy, increasing client trust*[1]

BACKGROUND

FINCA Azerbaijan, LLC, is a non-bank credit organization operating under limited license from the Central Bank of Azerbaijan that provides micro-credit to clients across Azerbaijan.

Since its launch in 1998, FINCA Azerbaijan has become the leading non-bank credit organization in Azerbaijan, serving more than 60 regions of the country with more than 150,000 active clients.

FINCA Azerbaijan shares in the common mission of FINCA International,[2] which is to provide financial services to the lowest-income entrepreneurs so they can create jobs, build assets and improve their living standards. FINCA Azerbaijan aims to be the institution that micro-entrepreneurs and small business owners turn to with their financial service needs. In order to be known and respected throughout the country, FINCA envisions becoming a permanent, sustainable financial institution with a nation-wide branch network.

FINCA is committed to providing the best possible service to clients to enable them to build successful businesses, while at the same time ensuring they are protected from unnecessary risk.

The largest microfinance institution in the country, FINCA Azerbaijan currently[3] serves more than 152,000 clients (31% women of December 2013) through 33 branches and 33 sub-branches throughout the country (see **Table 1** for key performance indicators).

FINCA offers loan products as group loans, individual loans, and rural and urban loans. Its target clients are those involved in trade, service, production or agricultural activities in rural and urban areas.

This case study has been written with a specific audience in mind: microfinance providers who seek to improve their practice in relation to specific standards of the Universal Standards for Social Performance Management (Universal Standards).[4] This case study provides a practical overview of the process of developing and implementing a client data privacy protection system in FINCA Azerbaijan. The case also provides recommendations on improving the effectiveness of the system in relation to the Universal Standards, as well as some general lessons for practitioners.

Table 1: Key performance indicators

Area/year	2010	2011	2012	2013
Clients (K)	97.8	119.8	136.9	152.8
Loan portfolio ($K)	82,007	114,745	149,620	210,869
PAR% (<30 days)	0.2%	0.2%	0.2%	0.25%
Women clients	34%	32%	32%	30.5%
Rural clients (%)	N/A	59.2%	58.5%	61.8%
Staff (total)	765	811	924	1,178
Staff turnover	14%	14%	19%	11.9%

Box 1: The Social Performance Fund

The Social Performance (SP) Fund for Networks[5] is designed to mainstream the new Universal Standards for Social Performance Management. The SP Fund works with 10 networks that run 18-month projects to document learning and experience around innovative solutions to implementing the essential practices of the Universal Standards. They also support their members to reach full or partial compliance with one or more dimensions of the Universal Standards. Supported by the Ford Foundation, the Fund is managed by the Microfinance Centre (MFC), a microfinance resource center and network serving the Europe and Central Asia region and beyond.

[1] Written by Sevda Huseynova (AMFA) with input from Zaur Nurmammadov (FINCA Azerbaijan), Kinga Dabrowska (MFC) and Katherine Knotts. Special thanks for Leah Wardle (Smart Campaign) for the diligent peer review of this case. For more information about AMFA's work, visit **www.amfa.az**

[2] FINCA International is a global network active across 22 countries

[3] As of December 2013

[4] The Universal Standards are management standards and practices for all MFIs pursuing a double bottom line. **www.sptf.info/spmstandards/universal-standards**

[5] More information can be found at **www.mfc.org.pl/en/content/social-performance-fund**

OVERVIEW

FINCA Azerbaijan prioritizes the safeguarding of client data privacy, not the least because it works with poor and low-income clients. This vulnerable segment of society is often reluctant to share their data, being unaware of their right to privacy. FINCA has witnessed cases where family members object to a relative seeking a loan, and the family conflicts that can arise when it transpires that the client did take the loan. The hesitation to share information also stems from clients believing that their data can be disclosed to their business competitors. Conversely, as client awareness around confidentiality increases, they are more demanding of their rights vis-à-vis the MFI.

FINCA views confidential information as any details related to the client's business or person that is not in the public domain, which is gathered by FINCA employees through their interactions with clients. This includes: loan amount, business sales data, household expenses, business strategy and other information that the client may not voluntary disclose to a third party. FINCA Azerbaijan's Client Data Privacy Maintenance system allows the organization to collect, use, distribute and store client information effectively and securely. The system is common to all FINCA offices around the world.

The loan contract includes an article stating that FINCA commits to keep all client data confidential, and to use it only for its normal business purposes. Client data can only be disclosed to third parties if the client has given their specific written consent upon request of FINCA management. Employees are allowed to share confidential information internally only at the request of their direct supervisor (e.g. even if internal audit asks for client data, loan officers can't provide it without permission). FINCA discloses data without client consent only where required by law (e.g. enquiries from the Centralized Credit Registry or court/government agency about the client), but only if sufficient legal proof supports the request. Additionally, client data may only be used the purpose it is gathered for. Finally, FINCA's legally-binding commitment to confidentiality applies to individuals and their businesses even when they leave the institution.

For FINCA, commitment to data privacy starts at the moment of hiring. All new employees sign a confidentiality agreement stating that the signer cannot disclose proprietary knowledge, product information, strategic plans, and other information that is confidential and proprietary to the organization during and after their employment. This applies to all staff, no matter what their role.

Privacy of client data is described in the following internal policies and documents:

- **Lending Manual:** regulates and ensures adequate protection of client data provided to FINCA's lending staff.
- **Archive Procedures:** ensures protection for all hard copy documents
- **Finance Manual:** regulates use of loan files, protection of clients' loan file data.
- **Code of Conduct:** manages the behavior of employees, including commitments and sanctions with respect to client data privacy. It also describes what confidential information means for FINCA and how client information should be stored.
- **Staff employment contract and confidentiality agreement:** Legally assures employees' respect for the confidentiality and privacy of all data (of both clients and the MFI).

SOLUTION DETAILS

Implementing the client data privacy mechanism

Clients' electronic data privacy is maintained by robust IT systems and solutions. Since 2008, FINCA Azerbaijan has used FLEXCUBE Retail VCO 2.0.1 to increase the productivity of its operations. The main priorities of the system are the provision and protection of client's personal and financial information, safety and loyalty.

Who can access data?

Data privacy starts from the very first interaction with clients. Loan officers process application data and then transfer it to the Loan Committee or data entry staff. A dedicated MIS manual regulates data that is entered into the system by Data Entry Operators (DEOs). Each staff level has its own system entry login, the password for which changes every 30 days. There are clear

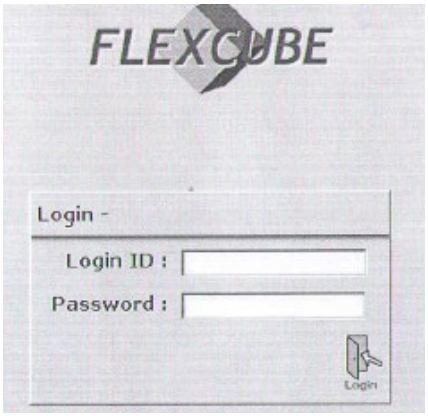
"The simplest, most conservative and most effective way to comply with the FINCA information confidentiality commitment is to avoid disclosing any information received from a client except the authorized fellow employees who are also working for the client." - FINCA's Code of Conduct

definitions around staff access to key MIS modules. Access is requested by HR and approved by the MIS department, and is restricted (by password) only to those modules relevant to the staff member's work. For example:

- **DEOs** have the broadest data editing authority, as they are responsible for entering data. However, DEOs have editing/data entry access to data specific to their own branch. New DEOs receive a username and password only after a one-week MIS training (provided by internal trainers) and relevant approval of managers based on a written letter of request. Access can be granted to employees during a probation period, and cancelled if they don't pass the probation period.
- **Loan supervisor** access allows them to review and approve loan amounts only within their own branches.
- The **accounting department** only has access to the accounting modules, and cashiers only to the cashier modules.
- **Department heads** only have access to the information that is relevant to their role. For example, head of Marketing Department can only see a client list, the HR manager can only access modules regarding employees. When departments have extraordinary client data requests, access is subject to approval of a written request to the MIS department (copying the CEO or head of internal control).
- **Archivists** can only add files to the database of their own branch.
- Only two people have the right to delete any document from the system: the **Document Controller** and the **IT manager**. The IT system produces a report on deleted files showing file name, date of deletion and the person who deleted it. Loan officers have access to the electronic archive of the client loan files, with no permission for deletion or edition.
- **Loan officers** are only allowed to print 3 files from the client folder: the loan application, repayment schedule and contract. The IT system also flags when a client's file is reviewed by a loan officer more than 5 times a week — as a safeguard against fraud.

In general, FINCA's IT system meets national banking requirements. It has strong firewall system that protects the system from unauthorized access. Remote access is only granted to senior staff based on written permission from their line manager and the head of the IT department.

Figure 1: FLEXICUBE login screen



Remote access is managed through the remote access terminals and valid for the period of request only.

Where is data stored?

The loan manual states that hard copy client data will be kept as required by national legislation.

Hard copy documents are stored in the archive. There are archive rooms (with 1 archivist each) in every branch. In addition, since 2010, there are 3 Regional Archives in the regional offices and one more regional archive is under construction.

After loan disbursement, cash desk submits a complete loan file to the archivist who reviews its completeness and registers it in the log book, which is signed both by the archivist and the loan officer. The log book includes the name of branch, date, name of receiver, name of file, name of client, as well as dates and signatures for each instance the file is moved in and out of the archive. Received files are placed into the shelves according to the alphabetical order.

Recent improvements to the archival system include the digitization of all hard-copy client files, to improve data security and facilitate the search for old/new client files. A separate data server stores all scanned documents.

Archive rooms are equipped with non-transparent windows. Archive room keys are kept by two persons in the branch: archivist and branch manager (in case the archivist unavailable). When the archivist is unavailable for less than a day, documents are kept by the Treasurer. For longer absences, documents are kept by Data Entry Operators pending the branch manager approval. All archive rooms are supplied with fire extinguishers and smoke detectors.

Figure 2: Document storage (before and after)

Non-active loan files are sent from branches to the regional archives for safe storage. The destruction of the non-active archived documents is completed in line with the national legislation.[6]

Raising client awareness

Before loan disbursement, field staff must read the entire loan agreement, and explain the client confidentiality clause, to the client. As part of this, the employee is required to check whether the client fully understands their rights to confidentiality. At the end, the client is required to sign a special form to affirm that he/she understands every aspect of the contract. FINCA also provides clients with detailed written information about data privacy and confidentiality in the loan agreement form.

Training staff

Each new employee receives the following documents:

- **Statement of Mutual Agreement:** the employee agrees to read the HR Manual and affirm understanding by signing a document.
- **Confidentiality Agreement:** states that the employee will not abuse client confidentiality, defines types of confidential data, data completeness and other operations. This is signed by the employee.

During orientation training, one full day is devoted to standards of business conduct, including maintaining client data privacy. Employees read all client service standards beforehand and upon arrival sign a statement to affirm they have read all the client services standards, code of conduct and confidentiality statement. During the training, different examples based on real cases are presented to employees for discussion.

There is also an annual "refresher" training for all staff, in line with FINCA International's requirements. Within one month of this, all branches hold "refresher" roundtable discussions on client service standards. To increase the efficiency of this (due to increasing staff numbers), in 2013 FINCA Azerbaijan started conducting refresher training and testing online.

All staff members have permanent access to all HR Manuals to improve their knowledge and skills on confidentiality, safety and conflict of interest issues, which in its turn that staff always have access to the latest information. Data privacy issues are also constantly discussed with employees during various trainings, meetings and roundtable discussions.

Getting client consent

In order to publically use a client's photo, data and/or success story, FINCA gains written approval from the client using a consent form signed during the loan disbursement, which is also co-signed by a witness confirming that client signed it after understanding its content. This form written in simple language, stating:

"By the below signature and fingerprint, I authorize FINCA Azerbaijan to use my story and photo by FINCA and its authorized representatives for the purpose of editing, printing, trade, upon donor request in microfinance promotional campaigns and for microfinance audiences of any form. By this, I waive any claim against FINCA regarding the requirement and liabilities for using my story and photos. I understand that, FINCA can use my story and photos for advertising, representation, web page and web promotion, and for other reasons defined by FINCA. This permission will be valid until they provide written letter to withdraw it."

FINCA regularly submits client data to the Centralized Credit Registry (CCR) and also receives client data as part of the loan check process. For this, FINCA uses a form to inform clients about how their data from the CCR is used. Client consent is not required to submit client data to the CCR.

[6] According to law, HR documents should be kept at least 75 years, and client documents should be kept at least 5 years. FINCA signed an agreement with the Waste Exploitation Factory around burning abolished files. To date, financial documents never been destroyed in FINCA. FINCA recently started to destroy client files that are not active for over 10 years, with the approval of the Country Director and with notification to FINCA International.

System monitoring and sanctions

Data confidentiality protection compliance is checked by Internal Audit (IA) and Internal Control departments (CD). As part of their spot check and audit rotation, they check branch-level document control effectiveness up to four times annually. If in the interim a client complaint around confidentiality emerges, it is investigated immediately by IA and CD.

In line with their clear commitment to client data confidentiality, FINCA Azerbaijan includes language around this issue in its Code of Conduct. In this way, if client data confidentiality is violated by an employee – civil, administrative or/and disciplinary measures can be taken depending on the result. Several specific disciplinary measures apply (reprimand, severe reprimand and dismissal) and have been acted upon in the past in case of privacy breaches. A Disciplinary-Administrative Committee investigates reasons (i.e willing or unwilling) for privacy breaches, discusses these with the employee and issues a decision on the sanction (e.g. warning letter, termination).

IMPROVING THE SYSTEM

There are a number of ways to bring FINCA Azerbaijan's client data privacy mechanism more in line with the Universal Standards for Social Performance Management. These are:

- FINCA should consider tracking privacy breaches on an annual basis to identify areas for improvement.
- Include guidance in the lending manual and other relevant policies on how to engage clients in discussions on the topic of data privacy. This could include training materials and sample dialogues for frontline staff to read clients out loud to cover the client's right to privacy, and the responsibilities of both FINCA and the client. Consider adding an "ethical dilemma" exercise to orientation training

Table 2: Level of effort required to maintain the system

Position	Role in brief	Time
MIS Administrator	Ensure MIS data integrity and system functionality Ensure that all MIS processes (end of day, beginning of day) run smoothly Ensure correct modifications or additions to the existing parameterization required by policy changes Perform daily system monitoring, verify integrity and availability of all hard-ware, server resources, systems and key processes, review system and appli-cation logs, and verify completion of scheduled jobs such as backups. Maintain access profiles and levels for different staff Enable remote system access as required	>60 % of a full-time post
Helpdesk Officer	Provide in-house expertise in FLEXCUBE functionality and reporting infra-structure Provide functionality support to the FLEXCUBE end-users Provide system passwords and logins Issue requests for password changes Troubleshoot access issues Enable remote access to the system as required	> 80% of a full-time post
Document Control Officer	Organize, keep and control documents in line with procedures Control electronic archive Control the confidentiality of archive documents Destroy archived documents Document incoming and outgoing archive files Updating and changes to the archive procedures, forms and policy; Branch visits, trainings, and discussions on archiving	Full-time post

that demonstrates the risks of breach of confidentiality.

- Although the loan contract includes a statement about informing clients about accessing their data from the CCR, it should also state that FINCA can submit client data to the CCR.
- FINCA should train its lending group leaders to safeguard group member information, particularly saving account balances, dates of loan disbursement, and information on repayment problems.

LESSONS LEARNED

A number of lessons emerge from FINCA Azerbaijan's work around client data protection, which are of interest to a broader set of stakeholders. These are:

Buy-in and commitment from senior management is critical. Without this, staff will place little importance on protecting either client or institutional data. Support this commitment with measures to fully implement data protection systems, train staff and raise client awareness.

Ensuring commitment of your staff is a second challenge: staff should understand, accept and respect the policy/procedures for the system to succeed. As front line staff form the main point of contact with clients, their full compliance is crucial for success.

Raising clients' awareness of their right to data privacy, and the MFI's responsibilities to ensure this, is vital. A responsible MFI should clearly communicate to clients their rights and be sure the message is understood; not only will this help with fraud detection, but it might convince clients to bank with an institution that actively protects their rights.

Invest in solid technology, if you are financially viable. Strong IT systems are a key asset to data privacy protection. As your institution grows, controlling/ supervising privacy protection of both institutional and client data becomes challenging, and the right IT system can help facilitate data documentation and protection. It will also protect against unintentional data abuse by staff (e.g. by password protecting data modules by staff level, and tracking data access patterns).

For more information:

FINCA Azerbaijan: **www.fincaazerbaijan.com**
FINCA on the MIX: **www.mixmarket.org/mfi/finca-aze**
Azerbaijan Micro-finance Association: **www.amfa.az**
The Microfinance Centre: **www.mfc.org.pl**
Social Performance Task Force: **www.sptf.info**

ANNEX 1: COMPARING FINCA'S CLIENT PRIVACY MECHANISM TO THE UNIVERSAL STANDARDS

Standard 4d: The privacy of individual client data will be respected in accordance with the laws and regulations of individual jurisdictions. Such data will only be used for the purposes specified at the time the information is collected or as permitted by law, unless otherwise agreed with the client.

	Essential Practice	Notes on FINCA's system
4d1	**4d.1 The institution has a privacy policy and appropriate technology systems.** IND 1) The institution has a written privacy policy that governs the gathering, processing, use, distribution, and storage of client information. The policy covers current staff as well as those who leave the organization and information leakage. (Y/N) IND 2) The institution's privacy clause is in plain language and not hidden in legalese or the contract. The privacy clause stands out and is not in small print. (Y/N) IND3) The institution's Staff Book of Rules and/or Code of Conduct penalize misuse or misappropriation of data. (Y/N) IND 4) The institution has penalties for exposing or revealing client data to third parties without prior client consent. (Y/N) IND 5) The institution has systems in place (including secure IT systems) to protect the confidentiality, security, accuracy and integrity of customers' personal and financial information. (Y/N)	Privacy-related clauses are included in various policies and written documents such as the Code of Conduct, Lending manual, Loan contract, MIS manual, Labour contract; and Archive manual. The privacy clause in the loan contracts is in clear language and not in small print. The Code of Conduct penalizes data misuse or misappropriation. Client consent is received from all parties. Using client data without client consent is penalized.

ANNEX 1: COMPARING FINCA'S CLIENT PRIVACY MECHANISM TO THE UNIVERSAL STANDARDS

	Essential Practice	Notes on FINCA's system
4d1	IND 6) The institution's IT systems in place have different password protection systems that are changed periodically with different access levels according to the position of the staff member accessing the data. (Y/N) IND 7) If files are stored in physical format, the institution stores the client files in a secure location, within the branch or headquarters that has a) restricted access only to selected persons; b) is kept in a facility secure from arson or theft. (Y/N)	Good systems are in place: strong protected MIS and IT systems, archiving procedures and conditions. Password systems are robust system passwords are different for each level of staff and are changed monthly. Staff access is limited only to the data that they need. Hard copy files are kept in an archive room in every branch and head office, with specially-assigned staff resources. Fire alarms and extinguishers are available.
4d2	**4d.2 The institution informs clients about when and how their data is shared and gets their consent.** IND 1) The institution has a policy (included in the training manual) to describe how to talk to clients about this topic. Requires that the institution present clearly to clients how it will use and share their client data. (Y/N) IND 2) The institution communicates well the privacy policy to staff. (Y/N) IND 3) The institution trains its staff to protect the confidentiality, security, accuracy and integrity of customers' personal and financial information. (Y/N) IND 4) The institution informs customers how their information will be used internally and, when applicable, when it will be shared externally. (Y/N) IND 5) Prior to loan disbursement, the institution's staff reads the privacy portion of the contract to the client. (Y/N) IND 6) The institution's contracts include a data privacy clause, describing how and when data can be shared (in addition to credit bureau information). (Y/N) IND 7) The institution requires written client consent to use information or photos in promotions, marketing materials and other public information. (Y/N) IND 8) The institution requires written client consent to share personal information with any external audiences, including credit bureaus, insurance agents, collection companies and others. (Y/N) IND 9) The institution trains group leaders to safeguard group member information, particularly saving account balances, dates of loan disbursement, and information on repayment problems. (Y/N)	Written policies don't include clauses on how to talk to clients about data privacy. New staff discuss the privacy clause during orientation. All staff sign a special form stating their commitment to protecting confidential data. During orientation, staff are trained on protecting the confidentiality of client data. Clients are told that FINCA request their data from the CCR; client consent to data/photo/story use is granted using a special form. Loan officers read the contract to the client, including the confidentiality clause. Contract includes a general privacy statement demonstrating the organization's obligation to respect client data confidentiality; a separate client consent form is attached to the contract. Contract doesn't include a statement for sharing client data with the CCR, neither does a special form (this just states that the organization can make an enquiry to the CCR to get information about him/her).