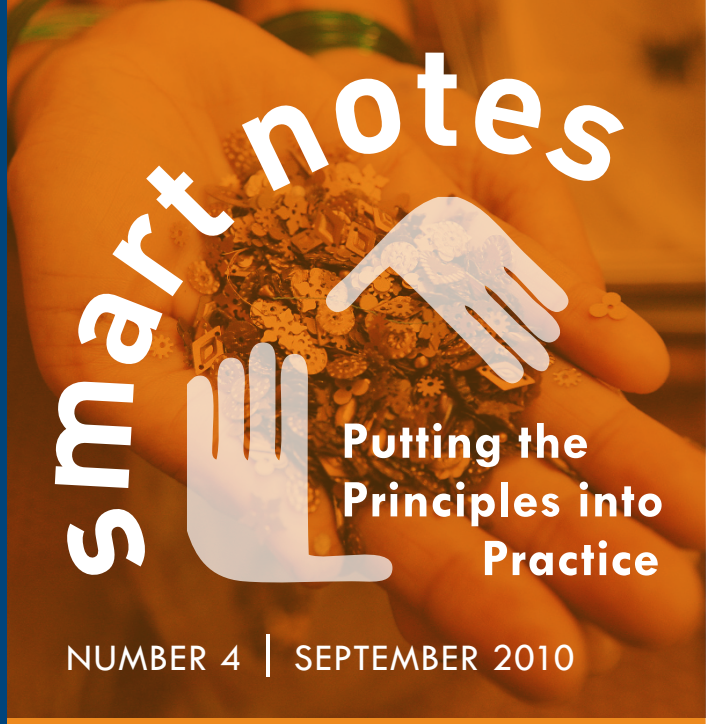

smart notes

Putting the Principles into Practice

NUMBER 4 | SEPTEMBER 2010

Privacy of client information requires both high quality data security protocols and diligence in maintaining the confidentiality of client information.

CAJA MORELIA VALLADOLID®
SERVICIOS FINANCIEROS
Desde 1964

Upon transforming to a regulated financial services provider, Caja Morelia needed to meet federal data management and reporting requirements. Faced with these new technology needs, Caja invested in a data management system and supporting processes to provide superior data security.

Customized IT at Caja Morelia safeguards client data

At Caja Morelia Valladolid, investing in high quality technology is the foundation for accurate and secure client information as well as the basis for strong customer service for its clients.

Caja Morelia began as a cooperative society initiated by the Catholic Church in 1964. In 2005, it became a regulated cooperative overseen by federal authorities in Mexico and by 2008, Caja Morelia had transformed into a regulated financial intermediary subject to national and international accounting standards. The cooperative owned by its 250,000 members, and all employees must be members, which keeps employee incentives aligned with member interests and enhances their commitment to customer service.

Upon transformation into a regulated financial service provider, Caja had to meet federal data management and reporting requirements. Instead of simply viewing this new technology as an additional cost of the transformation process, the management team at Caja saw an opportunity to invest in a customized solution that would provide superior data security and allow the cooperative to meet federal anti-money laundering requirements. The institution's history of developing its own systems and software enabled it to see the value of a customized solution for its new technology needs.

Caja spent three years developing its own data management system, one year creating the infrastructure necessary to support this system, and six months testing and refining it prior to launching the system as part of its transformation process in 2008.

The institution decided to hire in-house software engineers to create and maintain a custom client database due to several business advantages:

- Lower long-term cost by keeping maintenance in-house;

- More responsive technical support and faster issue resolution, resulting in less wasted staff time; and
- A customized system that fits the institution's needs and federal requirements exactly.

The database development process resulted in robust data management and security protocols. The in-house system is well integrated with the institution's other systems, and it meets the bank's specific data management and transaction monitoring needs.

IMPROVING INFORMATION QUALITY & MANAGEMENT

Caja Morelia's new legal status as a regulated financial service provider necessitated improvements to the quality and management of client information. Part of this process involved the creation of a single master electronic database with remote access for branch offices. Each branch can enter and modify the data for its clients, but cannot download the master database, preventing version control problems and limiting access to client data by branch staff.

Management at Caja recognized that the new database was only as valuable as the client data it contained. At the same time it was upgrading to the new system, Caja carried out its first cooperative-wide campaign to encourage its clients to update and correct their personal information. Many clients who had been with the institution for years had never updated their information—including several clients who had been with Caja since it was established in 1964! Caja's "We Want to Get to Know You" campaign offered prizes and rewards to encourage each member to update his or her information and bring in any documentation that was missing or outdated.

Although the process proved more time-consuming and difficult than management originally expected, Caja was able to update half of its clients' data in 2008 and almost all of the remaining clients in 2009, which has helped the institution reduce documentation errors, improve processing times, and have more personalized communication with clients. Additionally, the campaign helped create the kind of high-quality database necessary to prevent money laundering and effectively exchange information with the national credit bureau.

CONTROLLING ACCESS

Restricting access to the database and regulating data entry users and data modification users are key features of rigorous data security system. One of the most robust features of the data management system at Caja Morelia is the series of checks and balances that exist to prevent users from being able to carry out queries and changes alone. The database always requires that at least

two people, and often more people from different departments, authorize access or changes to client information.

At Caja, branch employees play an important role in verifying and updating member data on a daily basis. Branch staff can neither see nor change the data for clients in other branch locations. In contrast, staff at Headquarters can see data from all the branches, but cannot change any of the data in the client profiles.

Each person who accesses the database uses an individual username and password. Users must change their passwords every four months and cannot repeat previous passwords. Whenever an employee logs into the database, their name, the information they query, and the time when the request is made, are all recorded in a query log. Headquarters employees enter and leave the main office using a thumbprint scanner and sign in process to prevent unauthorized access to the client information stored there.

Additionally, each computer is configured to access the system only from the department where its principal user is staffed. For example, a computer configured for a person in the Human Resources department cannot be used in the Accounting department. This practice helps prevent the unauthorized transfer of information between departments.

Caja has also ensured the security of their "mobile" operations. Mobile Tellers—bank tellers on motorcycles who use Palms to make transactions in the field—have only limited access to the master database. A small portable printer creates transaction receipts for the clients, while the teller must begin and end each day by synchronizing his Palm with the master database at his home branch.

Finally, Caja employs a full time "internal hacker" to constantly test the system's security. The programmer tries to break into the bank's systems from the outside, to access client information, and to undermine the bank's security systems. By constantly testing its systems, the bank stays one step ahead of external hackers.

HOW TO: SECURE DATA MANAGEMENT

Caja Morelia combines the following elements to maintain strict data security and privacy of client data:

1. High quality hardware
2. Internet and antivirus protection
3. Data Integrity
    - Helpdesk
    - Frequent Backups
    - Version Control
4. Custom software development
5. Database management
    - Specific user permissions
    - Frequently changed passwords
    - Limited editing capability

MAINTAINING DATA INTEGRITY

Caja Morelia uses a combination of hardcopy, digital, onsite, and offsite backups to maintain client information in the event of a system failure, natural disaster, or other emergency. The bank keeps clients' physical files at the branch that received the initial loan application. However, employees also scan the contents of the file

(application, contract, etc.) and upload it into the master database. This digital copy is linked to the client's profile, along with any other supporting documentation. Caja maintains the hardcopies of ex-client data for ten years before destroying them to meet legal requirements.

The system backs up the master database three times a day—in the morning, at midday, and after the close of each business day. This makes it unlikely that the bank would lose more than four hours of work in the event of a system failure. The backups are copied to tapes, which are stored in safes, one located at Headquarters and one located securely offsite. Only the General Manager and Head of Database Management can access these safes.

GOOD PRACTICES IN CLIENT PRIVACY

Beyond building a strong IT system, Caja Morelia also maintains practices that ensure the privacy of client data throughout its operations.

The institution requests written permission from each client for the use of his or her image, story, and/or name on any marketing materials that the bank creates using that personal information.

During the collections process, the bank makes sure only the collections agent, branch manager, and headquarters Collections Department has access to personal information for clients with overdue loans. When the bank uses a specialized external collections firm, it shares only the few pieces of information that are most necessary for the firm to recover the loan.

All Caja employees sign confidentiality agreements with the bank as part of their employment contracts. In-house software developers also sign contracts to protect the proprietary nature of the software. The bank can bring criminal charges for violations of these agreements.

LESSONS LEARNED

The main lessons learned from Caja Morelia's experience include:

- Building an in-house database gives the institution a customized system that meets their specific needs and can be maintained by their own staff.
- Updating client records is a large task but produces better security for clients and improved communications with clients.
- Employing an "internal hacker" keeps an institution a step ahead of external hackers and pushes them to continually improve their data management system.
- A clearly defined user access hierarchy and frequently changed passwords help prevent institutional misuse of client data.

For more information on Valladolid's data security systems, please contact Homero Ambriz, Head of Systems and Monitoring, at his email: homero.ambriz@cajamorelia.com.mx *or Rodolfo Iñiguez Rosas, Gerente Comercial, at his email:* rodolfo.iniguez@cajamorelia.com.mx

By: Cara Forster
With special thanks to Alexandra Annes da Silva and Nick Wolf for their invaluable assistance.