TECHNOLOGY CONSULTING
IN THE GLOBAL COMMUNITY

Final Consulting Report

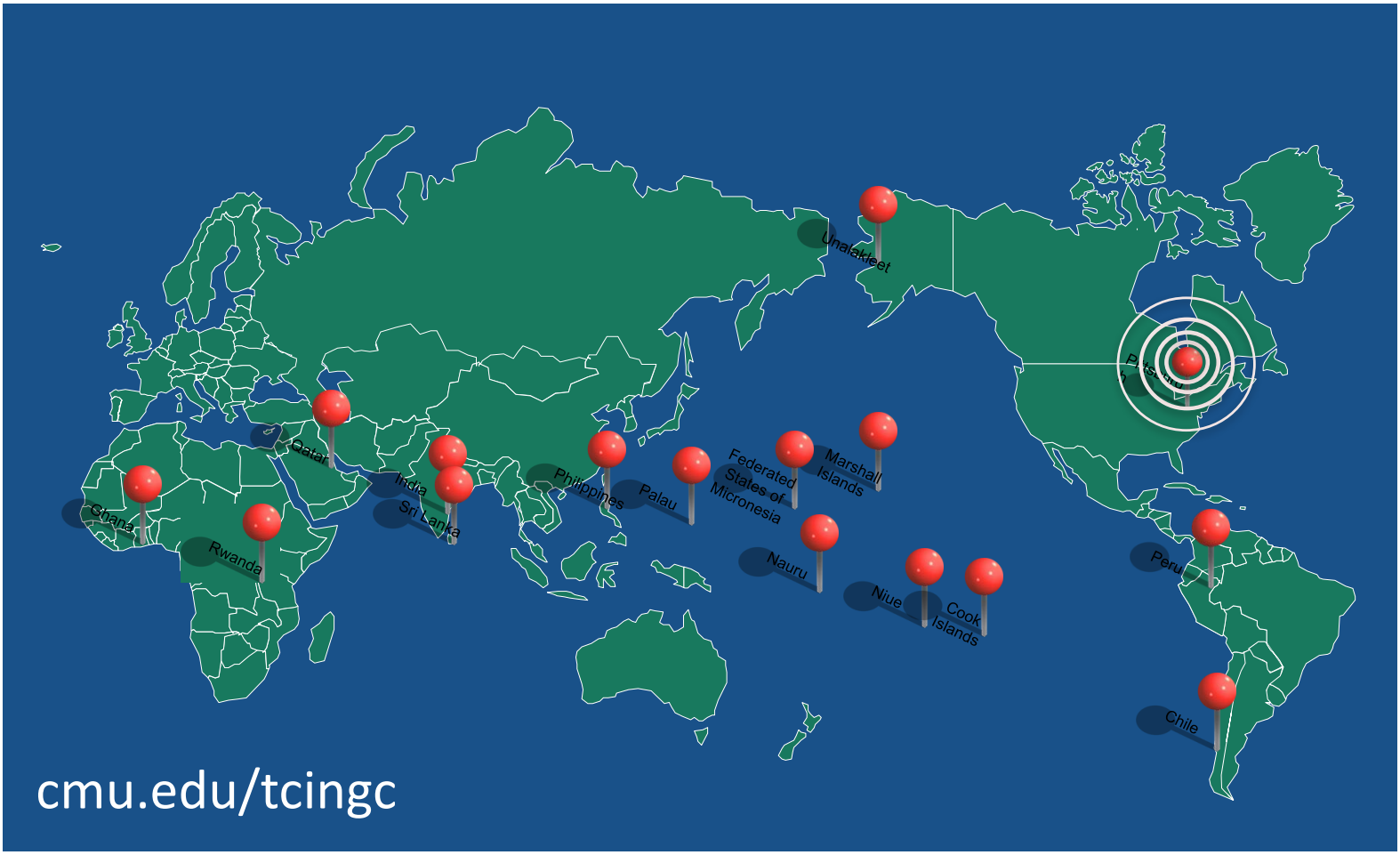
Banking Commission

Republic of the Marshall Islands

Jibby Ayo-Ani & Matias Quintana

August 2016

Carnegie Mellon University



cmu.edu/tcingc

Republic of the Marshall Islands

Banking Commission
Executive Summary

Student Consultants, Jibby Ayo-Ani and Matias Quintana
Development Partner, Sultan Korean

I. About the Organization

The Republic of the Marshall Island Banking Commission is the lead agency for Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) in the Republic of the Marshall Islands (RMI) on Majuro Atoll. The Banking Commission has the powers of a financial intelligence unit (FIU), as a law enforcer over licensed banks, and as an AML/CFT supervisor of banks, financial institutions, and cash dealers. The mission of the Banking Commission is as such:

> *To regulate the financial system for safety soundness and to deter money laundering and terrorist financing and secure access to the global financial system.*

They currently receive financial information, Cash Transaction Reports (CTRs), Suspicious Activity Reports (SARs), and Regulatory Return Reports, from financial entities, including two banks, Bank of Guam (BOG) and Bank of Marshall Islands (BOMI). The problem with the current document submission process is that they are turned in by paper, so reporting entities must walk or drive over the documents to the Banking Commission daily. The information from the reports are then entered by hand into a single Microsoft Excel spreadsheet. The Banking Commission also has a relationship with enforcement to inform them about suspicious activity.

II. Improve Data Collection and Analysis

The current data collection process can be tedious and takes time away from the analysis of anti-money laundering and countering financing of terrorism. We created a process for reporting entities to submit CTRs and SARs to the Banking Commission (BC) electronically and then store the data in a database. This will allow a smoother process for the reporting entities to submit their documentation and for the BC to more regularly analyze the data for suspicious activity.

We have used an encrypted email, which the banks will securely send the CTRs and SARs to the BC. Then, the BC can upload the reports to the Microsoft Access database that we set up. The BC staff will be able to perform queries to the database, perform financial intelligence analysis on the data submitted, and additionally generate and send reports to law enforcement, in a concise and electronically secured fashion.

It is recommended that the BC Staff continue to utilize Microsoft Office 2007 and Windows 7 as migration with a program update may cause interference in the process. It is also recommended for the BC to hire more hands, as there are now 15 years of backlogged paper documentation that needs to be manually inputted into the database for the full scale analysis to yield true irregularities.

III. Inform the Public About the Banking Commission and AML/CFT

The transfer of information such as new regulations or news that the BC would like to share with the public is currently shared by word of mouth. A website would allow for communication to other financial entities and cash dealers that otherwise has not been present in the past. The website would provide information about new regulations, rules, and different news that should be shared with external parties and the general public.

We have created a Wordpress account to utilize as a Content Management Tool and a Bluehost account to create a website with the domain name www.rmibankingcomm.org. To ensure that the site is sustained, the BC must keep the website up-to-date and pay for the Wordpress account on a yearly (after the first 3 year payment) basis. The biggest risk is the website becoming outdated so the BC staff must regularly update the website to include new information and regulations.

We recommend the new IT person hired upkeep of the website, and ensuring that all payments are met. Additionally, to make sure the website is seen by reporting entities sending them an email of the new website and printing the website address on future business cards would allow for a more widespread knowledge of its existence.

IV. Improve Security and Reliability of Banking Commission Email Communication

The email servers that the BC uses do not require secure message transmission (i.e. TLS) therefore email messages can be intercepted and the confidential information disclosed. Organizational email addresses will help the BC have better control about information being shared.

A Bluehost email account was created, linked to the domain purchased for the informational website. To provide further security measures, such as encryption, the email was linked with a local application of Microsoft Outlook. The bank will use the admin email account to submit encrypted CSV files. This email should be the primary email used by the BC to ensure the security of sensitive information exchanged within the office and externally.

Development Partner

Sultan Korean
skorean@rmibankingcomm.org

RMI Banking Commission
http://www.rmibankingcomm.org

About the Consultants

Jibby Ayo-Ani
jibbyani@gmail.com

Matias Quintana
mquintan@andrew.cmu.edu

Republic of the Marshall Islands
Final Consulting Report

Student Consultants, Jibby Ayo-Ani and Matias Quintana
Development Partner, Sultan Korean

I. About the Organization

Organization

The Republic of the Marshall Island Banking Commission is the lead agency for Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) in the Republic of the Marshall Islands (RMI) on Majuro Atoll. The Banking Commission reports to the Minister of Finance, the Honorable Brenson Wase, and has the powers of a financial intelligence unit (FIU), as a law enforcer over licensed banks, and as an AML/CFT supervisor of banks, financial institutions, and cash dealers. The definition of a cash dealer, taken from the Marshall Islands Revised Code Banking Act of 1987 is:

> *"(i) a person who carries on business as an insurer, an insurance broker or intermediary, a securities dealer or futures broker;*
>
> *(ii) a person who carries on a business of dealing in bullion, of issuing, selling or redeeming travelers' checks, money orders or similar instruments, or of collecting, holding and delivering cash as part of a business of providing payroll services;*
>
> *(iii) an operator of a gambling house, casino or lottery;*
>
> *(iv) a person carrying on the business of currency dealer or exchanger."*[1]

The mission of the Banking Commission is as such,

> *To regulate the financial system for safety soundness and to deter money laundering and terrorist financing and secure access to the global financial system.*

They currently receive financial information, Cash Transaction Reports (CTRs), Suspicious Activity Reports (SARs), and Regulatory Return Reports, from two financial entities, specifically two banks, Bank of Guam (BOG) and Bank of Marshall Islands (BOMI).

Currently, there are only two entities submitting CTRs and SARs to the Banking Commission. CTRs are turned in everyday but SARs are less frequent, with 200 being turned in 2015. New leadership in the Banking Commission has made it a priority to improve AML/CFT regulatory reporting by the banks. With enhanced compliance enforcement, the number of SARs are expected to increase significantly.

New legislation is now being worked on by an Anti-Money Laundering Risk Management Consultant to decree a more solidified enforcing protocol. A new addition will be a Currency

[1] Taken from the Banking Act 1987, http://rmicourts.org/doc/pdf/MIRC_2014/VOL_1/TITLE%2017/Ch.%201%20-%20Banking%20Act%201987.pdf

Declaration Report, that will require Customs to file whenever cash over $10,000 is brought into or leaves the RMI.

The problem with the current document submission process is that they are turned in by paper, so reporting entities must walk or drive over the documents to the Banking Commission daily. The information from the reports are then entered by hand into a single Microsoft Excel spreadsheet. The spreadsheet is shared within the Banking Commission via personal email, which could pose a threat to the security and confidentiality of the information.

Not only does the Banking Commission have a relationship with banks, financial institutions, and cash dealers but also law enforcement. The information provided by the banks is utilized in two ways.

1. To regularly collect and analyze enough information for the Banking Commission to notice irregularities and then volunteer information about that suspicious activity to law enforcement.
2. To respond to law enforcement requests by providing information and analysis to support their investigations.

Therefore the Banking Commission needs the capability to:

1. Collect and archive information
2. Regularly analyze the information for suspicious activity
3. Conduct analyses requested by law enforcement
4. Generate reports from their analysis

The organization currently has five team members. Sultan Korean, the Bank Commissioner; Rendy Johnny, the Financial System Supervision Division (FSSD) Manager; Matthew McGuire, the Financial Crime Consultant; Samelda Leon, the Commissioner Office Supervisor and Domestic Financial Intelligence Unit (DFIU) Analyst; and Matt Muller, the IT Technician for the office.

Facilities

The Banking Commission has an office on Majuro Atoll, capital of RMI, and is located on the second floor of a former apartment building. They use four units. Each unit has two or three small office-sized rooms, a bathroom, and a small kitchen with enough space for a large table. All of them have adequate lighting, and air conditioning to keep the climate controlled, and enough power outlets. The offices are divided as follows:

- Banking Commissioner office
- Assistant Commissioner and Financial System Supervision Division Manager office. This office also contains the networked office printer and WiFi access point
- Administration and Finance office. This is where most of the meetings with banks and financial institutions are held, and where external consultants work during they stay. It also has a second WiFi access point.
- Domestic Financial Intelligence Unit and Office Supervisor office.

In terms of security, all apartment units doors are locked as well as the front door every night at 6 p.m. However, there is no secure system (i.e. video surveillance, alarms) for after hours, but an

on-site person outside the apartment building guarding it. The Banking Commission staff are the only people with the keys.

Regulatory Responsibilities

The Banking Commission gathers the reports sent by the banks, financial institutions, and cash dealers, analyzes these reports for possible activities related to money laundering, financial terrorism, and off-site surveillance. The reports are as follows:

Cash Transaction Reports (CTRs)

The CTRs record all cash deposits and withdrawals of $10,000 or more from banks and are utilized during macro-analysis by any requesting government officials. The report has total amount of money in and out, the date, who made the transaction, and the bank it came through. Law enforcement officials may request from the Banking Commission any information, based on the reports received, when an investigation is being conducted on people of interest who are suspected of money laundering or financial terrorism.

Suspicious Activity Reports (SARs)

SARs are generated when any sort of suspicious financial activity such as a series of large transactions or financial transactions that do not make sense for the individual or organization. The key elements of the report include the suspect's personal information, the amount of money transacted, the bank it went through, the summary of the type of suspicious activity, and the resulting actions against the suspect.

Regulatory Return Reports

Regulatory Return Reports are monthly reports on the financial condition and performance of the entities. It allows for the Banking Commission to aggregate data for the purpose of assessing the performance of the economic industry as a whole.

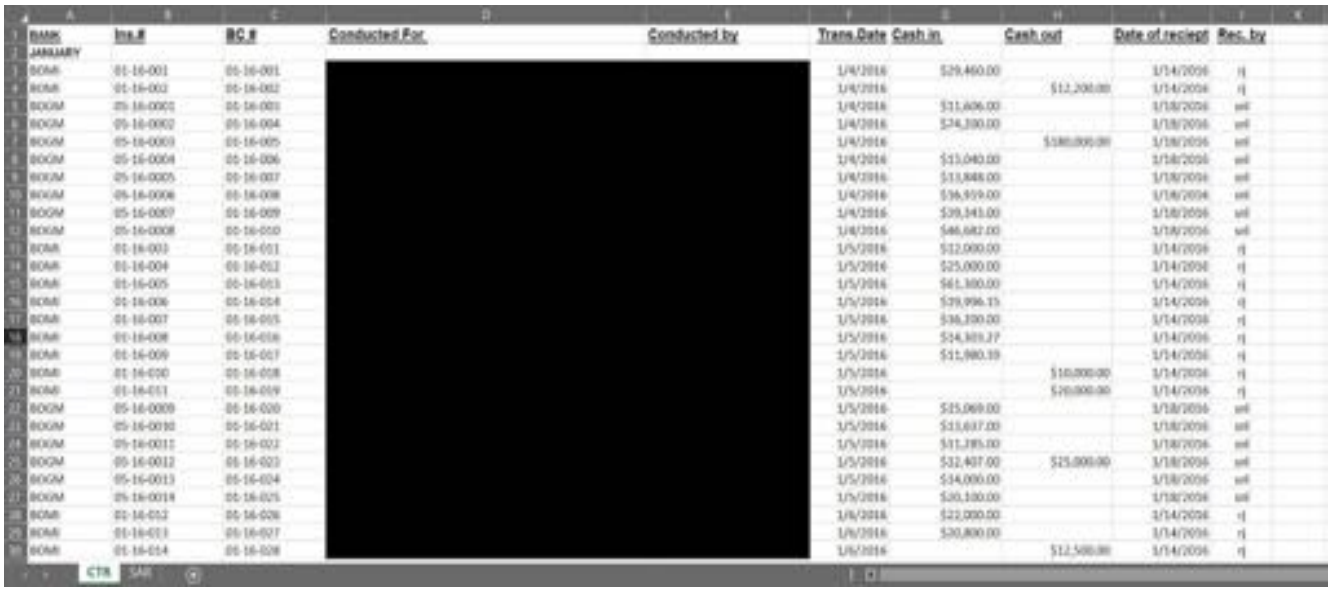
Currently the Banking Commission receives around 3,000 CTRs, 200 SRAs, and 80 Regulatory Return Reports on an annual basis from the two banks. Currently, the AML and Bank Secrecy Act Compliance (BSA) Supervisor from BOMI and the Operations Officer from BOG print out the reports and then walk or drive them to the Banking Commission's office. They are signed off by the Banking Commission office then the information from the reports are entered into a Microsoft Excel spreadsheet. One spreadsheet consists of information from CTRs and SARs (screenshot below), and another spreadsheet with Regulatory Return Reports information.

These spreadsheets are managed by Samelda Leon and Rendy Johnny, respectively. As a result, whenever Sultan Korean requires up-to-date information, Samelda Leon and Rendy Johnny have to email their current file. The original paper documents are then stored in file cabinets located in the DFIU office.

The entire process of managing the financial information is cumbersome. As mentioned before, the duty of manually recording the paper reports and performing the intelligence analysis is solely done by Samelda Leon and Rendy Johnny. As a result, a considerable amount of time is being invested in the manual process of retyping the information needed and not enough time for detailed intelligence

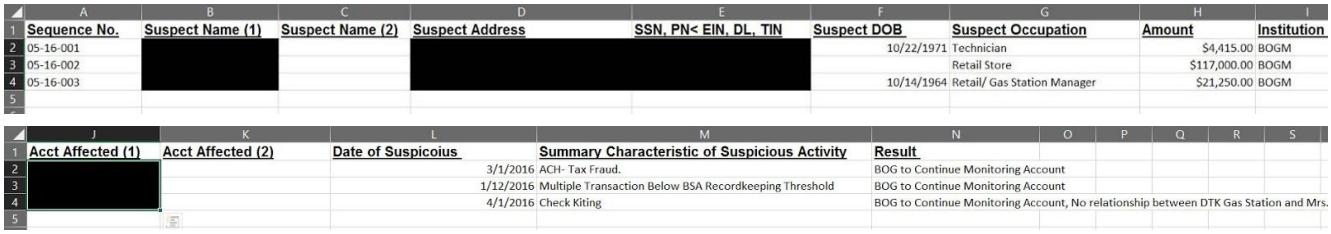
analysis. The Banking Commission would prefer to spend less time doing data entry and dedicate more time to intelligence analysis.

CTR spreadsheet used in the Banking Commission



BANK	Ins.#	BC #	Conducted For	Conducted by	Trans.Date	Cash in	Cash out	Date of reciept	Rec. by
JANUARY									
BOMI	01-16-001	01-16-001	[redacted]		1/4/2016	$29,460.00		1/14/2016	rj
BOMI	01-16-002	01-16-002			1/4/2016		$12,200.00	1/14/2016	rj
BOGM	05-16-0001	01-16-003			1/4/2016	$31,606.00		1/18/2016	wl
BOGM	05-16-0002	01-16-004			1/4/2016	$74,330.00		1/18/2016	wl
BOGM	05-16-0003	01-16-005			1/4/2016		$180,000.00	1/18/2016	wl
BOGM	05-16-0004	01-16-006			1/4/2016	$11,040.00		1/18/2016	wl
BOGM	05-16-0005	01-16-007			1/4/2016	$13,848.00		1/18/2016	wl
BOGM	05-16-0006	01-16-008			1/4/2016	$36,959.00		1/18/2016	wl
BOGM	05-16-0007	01-16-009			1/4/2016	$39,343.00		1/18/2016	wl
BOGM	05-16-0008	01-16-010			1/4/2016	$46,682.00		1/18/2016	wl
BOMI	01-16-003	01-16-011			1/5/2016	$12,000.00		1/14/2016	rj
BOMI	01-16-004	01-16-012			1/5/2016	$25,000.00		1/14/2016	rj
BOMI	01-16-005	01-16-013			1/5/2016	$61,300.00		1/14/2016	rj
BOMI	01-16-006	01-16-014			1/5/2016	$39,996.15		1/14/2016	rj
BOMI	01-16-007	01-16-015			1/5/2016	$36,200.00		1/14/2016	rj
BOMI	01-16-008	01-16-016			1/5/2016	$14,303.27		1/14/2016	rj
BOMI	01-16-009	01-16-017			1/5/2016	$11,980.39		1/14/2016	rj
BOMI	01-16-010	01-16-018			1/5/2016		$10,000.00	1/14/2016	rj
BOMI	01-16-011	01-16-019			1/5/2016		$20,000.00	1/14/2016	rj
BOGM	05-16-0009	01-16-020			1/5/2016	$15,069.00		1/18/2016	wl
BOGM	05-16-0010	01-16-021			1/5/2016	$13,617.00		1/18/2016	wl
BOGM	05-16-0011	01-16-022			1/5/2016	$11,285.00		1/18/2016	wl
BOGM	05-16-0012	01-16-023			1/5/2016	$12,407.00	$25,000.00	1/18/2016	wl
BOGM	05-16-0013	01-16-024			1/5/2016	$14,000.00		1/18/2016	wl
BOGM	05-16-0014	01-16-025			1/5/2016	$20,100.00		1/18/2016	wl
BOMI	01-16-012	01-16-026			1/6/2016	$22,000.00		1/14/2016	rj
BOMI	01-16-013	01-16-027			1/6/2016	$20,800.00		1/14/2016	rj
BOMI	01-16-014	01-16-028			1/6/2016		$12,500.00	1/14/2016	rj

SAR spreadsheet used in the Banking Commission



Sequence No.	Suspect Name (1)	Suspect Name (2)	Suspect Address	SSN, PN< EIN, DL, TIN	Suspect DOB	Suspect Occupation	Amount	Institution
05-16-001	[redacted]		[redacted]		10/22/1971	Technician	$4,415.00	BOGM
05-16-002						Retail Store	$117,000.00	BOGM
05-16-003					10/14/1964	Retail/ Gas Station Manager	$21,250.00	BOGM

Acct Affected (1)	Acct Affected (2)	Date of Suspicoius	Summary Characteristic of Suspicious Activity	Result
[redacted]		3/1/2016	ACH- Tax Fraud.	BOG to Continue Monitoring Account
		1/12/2016	Multiple Transaction Below BSA Recordkeeping Threshold	BOG to Continue Monitoring Account
		4/1/2016	Check Kiting	BOG to Continue Monitoring Account, No relationship between DTK Gas Station and Mrs.

Staff

The Banking Commission has four personnel.

- Sultan Korean is the Banking Commissioner. He manages the office and is the liaison with national and international financial entities. Additionally, as he builds the Banking Commission staff, he is directly involved in DFIU and FSSD intelligence analysis. Currently he uses a desktop computer for sending and receiving emails as well as Microsoft Excel for analysis and monitoring.
- Rendy Johnny is the FSSD Manager. He has a banking and accounting background and is in charge of monitoring banks' financial data. Currently he receives Regulatory Return Reports on a monthly basis in paper form and manually enters and tracks them in a Microsoft Excel

spreadsheet. Similar to Sultan Korean, he mainly uses his computer for email communication and using Microsoft Office.

- Samelda Leon is the DFIU Analyst. She receives CTRs and SARs in paper form and updates a spreadsheet with the new information. She later analyzes them and informs Sultan Korean about any person of interest.
- Matt Muller is the recently hired IT Technician for the office. He will be in charge of all IT related tasks for the Banking Commission as well as the database, website, and email maintenance.

Additionally, a United Nations Financial Crime Consultant, Matthew McGuire consults remotely and visits periodically. Matthew McGuire is helping the Banking Commission to redesign and rewrite the banking legislation, as well as advise them regarding AML/CFT. He uses his Lenovo Thinkpad connected to an external monitor.

Technology Infrastructure

Hardware and Software:

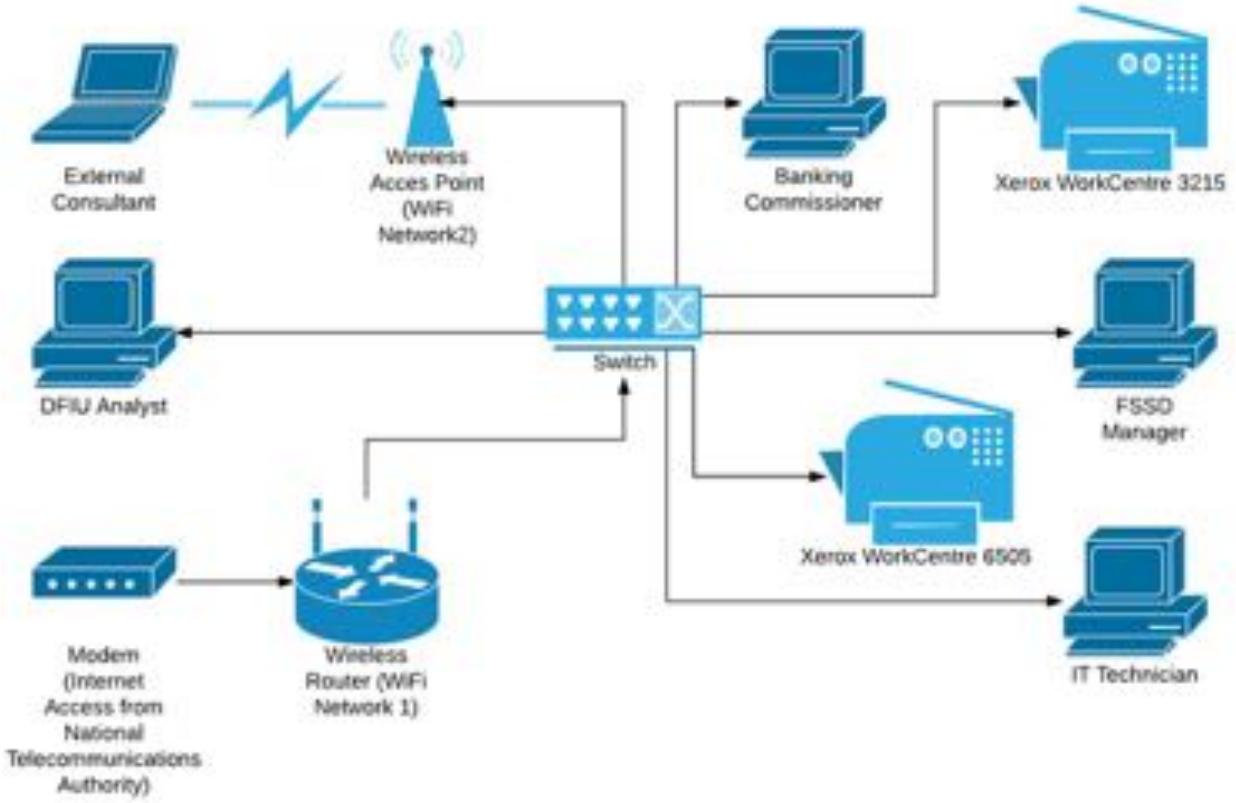
In the current situation, the specific technologies are described below in the table, although there are regular power outages that make the development partners vulnerable to situations such as losing data and ability to carry out the tasks for the day.

User	Hardware Equipment Specifications	Software Specifications
Sultan Korean Rendy Johnny Samelda Leon	Desktop Computer (one for each employee): - Model: HP ProDesk 405 G2 MT - CPU: AMD A4 6250, 2.00 GHz - RAM: 8.00 GB	- Windows 7 Professional Edition Service Pack 1, 64 Bits - Microsoft Office 2007 - Internet Explorer for browsing
Matt Muller	Desktop Computer - Model: Dell Inspiron 3847 - CPU: Intel Core i7 4790, 3.60 GHz - RAM: 16.0 GB	- Windows 7 Professional Edition Service Pack 1, 64 Bits - Microsoft Office 2007 - Mozilla Firefox for browsing
Matthew McGuire	Laptop Computer: - Model: Lenovo Thinkpad T460 - CPU: Intel Core i3-6100, 2.30 GHz - RAM: 4.00 GB	- Windows 10 Home, 64 bits - Microsoft Office 2007 - Google Chrome for email and browser

Banking Commission	Xerox WorkCentre 6505, Xerox WorkCentre 3215 (Multi-function devices)	

Network:

The Banking Commission have two WiFi networks but only one connection from the Internet Service Provider (ISP); there is an opportunity to join them into a single network. Both networks are WPA2 password protected and mostly used by consultants and advisors laptops when they go to the office, as well as other handheld devices. The following diagram describes the current devices attached to the networks, only laptops are connected wirelessly.



Network Diagram of the Banking Commission Office

Internet Connection:

There is only one ISP in the country, the National Telecommunications Authority (NTA), who manages the fiber optic connection from Guam to RMI. This allows for moderate speed connection for the basic household internet plan, around 1 and 0.6 Mbps of upload and download speed respectively, making streaming capabilities such as videos or Skype possible. However, in terms of bandwidth at the Banking Commission, the upload and download speed are around 0.10 Mbps. As a result, uploading or downloading large files takes a long time. Additionally, media streaming capabilities are very limited. There is a possibility for upgrading the current internet plan to enhance

the current situation. Lastly, there is a single undersea cable to RMI that limits the bandwidth and has been reported to be sometimes unreliable, leaving the island without redundancy.

Technology Management

There is currently no one responsible for managing the technology infrastructure at the office. Since they only rely on technology for email communication, office applications, and wireless printing, they did not required someone on staff to be responsible for it. Each staff member is responsible of updating their software and antivirus as needed. However, whenever they have a technology issue the RMI government has some IT staff that they can call for help. The Banking Commission has had IT problems in the past that has resulted in almost all historical data being lost. As mentioned before, a job position for an IT technician for the office is currently open.

Technology Planning

Sultan Korean does all the planning and budgeting including technology. His current vision is to use technology to minimize the amount of time and work required to archive and analyze all incoming reports from the financial entities and cash dealers. As a result, the FSSD and DFIU will become more efficient in their roles of monitoring and investigating. Additionally, Sultan Korean hopes that technology will provide visual tools to facilitate their day to day operations. A few FIUs in the region (Micronesia) collect electronic reports and store them in a database. He wants to similarly reduce the amount of paperwork in the office, as well as make information storage and analysis more efficient. Sultan is submitting a budget that will include expenditures for technology by the end of June so it would be ideal for him to have an idea of potential costs by then.

Communication

Currently, computers are being used mainly for communication purposes, such as email, and report analysis in Microsoft Excel. Information is shared internally through word-of-mouth, email, and externally via phone communication.

The paper reports from the financial entities are received by either Rendy Johnny or Samelda Leon, who records the information in Microsoft Excel spreadsheets. The spreadsheets are shared via email.

Each staff member has a personal gmail and ntamar email account that they use for communication. The latter is hosted by the NTA. The Banking Commission does not have a website nor domain for organizational emails.

As mentioned previously, the current method that the reporting documents are submitted is through pdfs that are filled out online then printed and walked over to the Banking Commission. This method is very inefficient because the bank workers have to take time out of their days to walk all the documents over, once a day, and then the Banking Commission must work to input this information into the computer by hand. This is a repeated action that has to be done everyday for as many documents that are turned in that day. This can lead to having too many errors, where possible inaccurate information being inputted or inconsistencies in titles, names, etc.

Business Systems

The Banking Commission reports to the Ministry of Finance and is part of the government. As a result, all business processes such as accounting and hiring go through them. The Banking Commissioner, Sultan Korean, will fill out the necessary paperwork and send it to its proper destination. They are currently in the process of establishing their Operational Statement and Budget for next year, which must be approved by the Minister of Finance, Honorable Brenson Wase.

The Banking Commission must also comply with international standards defined in the Financial Action Task Force 40 recommendations. These deal with the necessity to collect, analyze and disseminate information, and those that deal with international cooperation.

II. Improve Data Collection and Analysis

Motivation

The current way the Banking Commission collects data and conducts analysis is time intensive and leaves little room to ultimately catch and deter money launderers. The reports submitted to the Banking Commission are often inconclusive until a person's or organization's behavior is examined holistically to notice irregularities. To be able to look at the data as a whole, it would be most reasonable to have the information inputted into a database that then allows for a comprehensive analysis.

As mentioned before, with the current system, there are regular power outages and since there are desktops being used, data can be lost if changes have not been saved to documents being worked on. For that reason, we recommend a countermeasure for this sort of situation such as Uninterrupted Power Supply (UPS) or switch from desktops to laptops.

A further opportunity would be to visualize the data in a highly customizable data visualization software to automate, expedite, and increase precision in the current manual analytical process. Previously information is just kept in a Microsoft Excel Spreadsheet and analysis has just been inferred from the human eye. Larger trends from the information can be missed and a data visualization application or system from an already set up database would minimize the chance of data clean up and formatting issues.

Outcomes

1. Designed and Implemented Access database

After discussions and interviews with employees at the Banking Commission, the functional requirements were documented (see **Appendix A**). Additionally, three different options were evaluated (see **Appendix B**) and finally the first option "File Upload with Local Application" was recommended. This means that financial entities will send encrypted emails with their CTRs and SARs reports to the Banking Commission following the specified format (see **Appendix C**), and then the staff will upload those files to a local database.

For the locally hosted database, it was decided to use Microsoft Access. In terms of cost, the Banking Commission already had Microsoft Office Suite 2007 (with MS Access) installed on each computer in the office. The main decision factor was sustainability. Local existing technology solutions and technological skill on the island make this viable, as well as scheduled training for the recently hired IT Technician.

The database application contains 3 tables (see **Appendix D**):

- CTRs - Stores information about Cash Transaction Reports
- PersonInTransaction - Stores individual information about each person involved to a given CTR
- SARs - Stores information about Suspicious Transaction Reports

The database application contains the following forms (see **Appendix E**):

- MainForm
- CTRs
- SARs

The database application contains the following reports:

- CTRs by Person - A list of all people associated with a CTR, order by their identification number
- CTRs by Month - CTRs broken down by month with the sums for each month
- CTRs by Year - CTRs broken down by year with sums for each year
- SARs by Person - A list of all people associated with a SAR, order by their identification number
- SARs by Month - SARs broken down by month with the sums for each month
- SARs by Year - SARs broken down by year with sums for each year
- Crime Classification (SAR) - SARs broken down by summary characteristic with sums for each classification

And one plot of amount of CTRs by Financial Entity, grouped by month.

An original prototype of the database with all three tables (CTRs, PersonInTransaction, and SARs), related forms, queries, and reports. The prototype was presented to Rendy Johnny and Samelda Leon. They were able to test the reports, input data through the appropriate forms, and perform some queries. Through this testing, small bugs were detected and recommendations from the end users were captured. This was crucial for tweaking the design of the system as well as it allowed the employees to gain familiarity with the application.

During the development stage, the IT Technician Matt Muller was involved in the process in order to learn about the system. Test queries and reports were also performed by him in order to gain more familiarity with adding modifications to the system.

2. Documented and Set Up Electronic Reporting Process

As previously mentioned in **Appendix B**, financial entities will begin sending electronic reports via encrypted email to the administration email of the Banking Commission office. To gain a better understanding of the current reporting process of CTRs and SARs, meetings were held between the consultants and the IT team from Bank of Marshall Islands and Bank of Guam, as well as the AML Compliance teams from each bank. Because the paper forms will not be used anymore, it will be possible to get more data than just the required by the physical documents. However, a common ground of data fields needed to be set for both banks, and for future financial entities (see **Appendix C**).

During the final week of the project, banks are still finishing the last details of their electronic reports and have been sending test files. These files were uploaded to the database by Matt Muller and feedback was provided for both Bank of Marshall Islands and Bank of Guam. However, there is still the risk that the consultant will not be on island when the banks eventually submit their reports electronically. In addition, the banks do not yet have a timeline for when they will start the electronic submission, although it is expected to be in the next few weeks. In the meantime, backlog reports, as well as incoming paper form reports, will be inputted into the database manually. While this is tedious, it is a short-term solution until the banks submit their reports in the correct format. The Banking Commission is aware that this method cannot be sustained as a long-term solution as it creates more work for the employees. Nevertheless, once the reports are submitted in the correct electronic format, the amount of time inputting and sorting the data will decrease dramatically; this will leave more time for analysis and investigation. Finally, it is important for all previous reports (backlog) to exist in the database in order to provide a more thorough investigation.

3. Deployed Access database

In order to enable multiple users concurrently in the system, the database needed to be split into front-end copies and one back-end copy (see **Appendix F**). The back-end copy resides in Matt Muller's computer and front-end copies were distributed to each employee's computer. Using a Windows Homegroup, that was set up under the Banking Commission's network (see **Appendix G**), each user's front-end copy file was linked to the back-end database file (see **Appendix H**). In addition, this procedure helps to avoid the 2GB database file size limits of Microsoft Access (see **Appendix I**). Additionally, in order to increase the security of the system, both the back-end database file and the front-end files were encrypted using a unique password (see **Appendix J**).

After the final version of the database went live, Rendy Johnny and Samelda Leon had one week to manually enter data from previous reports and test the system. Rendy Johnny ran the reports as a test of what real-data will generate and was able to export them into excel spreadsheet for further analysis if needed. The ability of auto-completion in the text boxes, based on information already stored in the database, allowed Samelda Leon to input two complete reports in less than ten minutes. The banks were able to start sending test files with real CTR information, Samelda Leon and Matt Muller were able to upload the files (see **Appendix K**)and query the new data.

Backup procedures were discussed with Matt Muller, as well as worst case scenarios with the database. It was determined that he will set up a schedule for backing up the database, as well as received files from the financial entities, either once a week or after one set of reports is submitted.

Recommendations

In order for the project to be successful, and use the database in the most efficient way, it is crucial that the current banks and future financial entities properly reformat their reports to meet the guidelines necessary for automatic upload into the database. Since the banks are still in the process of testing their electronic reports, it is important to work side by side with them providing feedback and making sure their test files work as expected. While the solution of manually inputting all incoming reports is adequate for short-term, if it is used indefinitely, it diminishes the usefulness and efficiency of the new database. In order to accelerate the time of introducing old reports into the database, the Banking Commission could hire personnel, or have an intern, on an hourly wage to perform this task.

For future projects, there are many opportunities for growing and expanding the database. Additional visualization tools can be implemented within the database and Case Management Tools can be used with the database as a source. These projects could focus more in exploring and analyzing the data to further assist the office meet its goals. Additionally, reports that the FSSD receives, such as Regulatory Return Reports, can also be formatted into CSV files and be incorporated to the database in order to make all reports digital.

As the Banking Commission becomes more familiar with the database, it is possible they would like more reports and/or queries. The current IT Technician, Matt Muller, is capable of modifying the existing reports, as well as adding any new report they might need. However, additional training in Microsoft Access and databases would strengthen his skills. Finally, there is potential for automatic pattern detection, in order to help the office identify key entities or patterns of suspicious transactions. These projects can be implemented using Data Mining techniques and are feasible for a future TCinGC team or as a remote semester-long project from Carnegie Mellon University.

III. Inform the Public About the Banking Commission and AML/CFT

Motivation

Because there is no public centralized platform for all of the Banking Commission legislation for banks, cash dealers, and financial institutions to be up to date on, a website would be an added opportunity for the Banking Commission. Additionally, a website would help increase general knowledge of the issue of money laundering, and improve visibility of the Banking Commission's activities. Additionally, the website must be easy to maintain and update its content. The following table compares web hosting sites that allow changes to be made easily.

Outcomes

In addition to the domain name necessary for the website, it was determined that a website builder would give the BC the ability to sustain the website on their own. To determine what solution

would be the most cost effective, a diagram was created that compared the cost of the domain, hosting, and connecting with email. Wordpress fit the needs of the BC and was the most budget-effective solution. The BC selected an appropriate domain (www.rmibankingcomm.org) which was purchased through Bluehost. The website created on Wordpress contains 5 pages (see **Appendix N**):

- Home: A general landing page that gives a welcome message along with a brief description of the mission and purpose of the BC.
- About: A more detailed description of the BC, its mission, its organization structure, and its history.
- Legislation and Regulations: a list of all the current regulations and updated legislations.
- Contact Us: contains a form to submit a message (sent to administration@rmibankingcomm.org) as well as other contact information for the BC.

These pages contain information about the BC and its purpose in the community. The general public and reporting entities will now have easy access to the BC for any updates on legislation, important updates, and contact information. The BC can now more easily regulate the financial system for safety soundness and to deter money laundering and terrorist financing and secure access to the global financial system in the RMI.

While Wordpress is designed to be used by those who do not know how to program websites, it still requires the user to be familiar with Wordpress and the selected theme. After the website was built, the Banking Commission staff was walked through the most common functions such as updating a page, creating a post, and customizing the theme. However, these actions will most likely not occur frequently. This could become problematic when, in the future, the BC wishes to update or add information to the website, but has not done so recently. To help prevent this from occurring, documentation was created that details information about the site, as well as instructions on completing common tasks. In addition, there are plenty of resources online, such as at https://en.support.wordpress.com/, in case a more advanced feature is desired. Since the resources necessary to complete common and advanced tasks are available to the BC, maintaining the content to the website should be feasible. To ensure the website stays online, the BC simply needs to pay for the hosting plan once a year (starting after the first 3 year payment).

Recommendations

In order to continue to maintain the website, the BC needs to ensure they purchase the basic plan of Wordpress on Bluehost once a year. Since at the moment the BC office does not have a credit card, it is important that when they do, the payment method is changed to their new corporate credit card. To maintain the website up-to-date, it is important that all new legislations and regulations are posted under the “Legislation and Regulations” page, as well as any other information update, or

new pages if needed. This will reinforce the role of the website as a reliable source of information regarding the BC.

IV. Improve Security and Reliability of Banking Commission Email Communication

Motivation

As it was mentioned previously in the communication section, employees use different personal email domains. They recognize that this may not be ideal with confidential files being transferred through these emails. If an employee leaves the Banking Commission, confidential information and/or files will remain in its personal inbox creating a potential threat of information disclosure. Additionally, email services that do not use secure message transmission (i.e. TLS), like ntamar, can be intercepted. Finally, having an organizational email will promote the professionalism of the organization.

Outcomes

To help facilitate working with other FIUs, in addition to providing a professional means of communication, a Bluehost mail account was created and linked to the domain purchased for the informational website. Bluehost mail was selected because it provides 5 professional emails as part of their free plan, which fits the needs of the BC. To provide further security measures, the email was linked with a local application of Microsoft Outlook. Outlook allows a user to send digital signatures and send/receive encrypted messages. Outlook was set up on the desktop computers and laptops of all the BC employees. To assist the BC with setting up Outlook to allow encrypted messages to be sent for future employees, documentation was created that details necessary steps to configure Outlook appropriately. There is very little risk associated with sustaining the email. To ensure that Bluehost will continue to host the domain, it is important that the BC reads any emails sent by them about potential changes in pricing or plans. To ensure Outlook remains running, the BC has to ensure it completes any software updates or bug fixes sent out by Microsoft. Checks for these updates can be scheduled to occur automatically or after a set period of time (ex. once a week) under the ‘Help’ menu.

Recommendations

To ensure the use of the new organizational emails, Matt Muller could help the office migrating their address book from their previous email, as well as setting up auto-reply messages indicating the new email address. Additionally, contact information should be updated (i.e. business cards) in order to promote the new online presence of the BC (email and website).

V. Additional Recommendations

Banking Commission Understaffed Situation

The consultants recommend that the BC keeps prioritizing the completion of their new organizational chart. Prior, and during, the consultants stay, some meetings were postponed or delayed because the employees had other office tasks to carry on, not necessarily related to their job role. It is important to highlight that hiring the IT Technician while the consultants were in the office helped the capacity building process and training, but it would have been preferable if the person joined earlier.

About the Consultants

Jibby Ayo-Ani is a fourth-year student in Information Systems at Carnegie Mellon University. She has taken part in the Technology Consulting in the Global Community internship over the summer and return in the fall to start a promising career as a software developer at Capital One.

Matias Quintana is a graduate student in the Master of Information Systems Management in the Heinz College at Carnegie Mellon University. He will be returning to Carnegie Mellon University in the fall to finish his program following the Technology Consulting in The Global Community internship over the summer.

List of Appendices

Encrypted Email and Local Application

Informational Website

Professional and Secure Email

Appendix A.

Functional Requirements of Solution

- A system by which the financial entities can electronically file CTRs (Cash Transaction Reports) and SARs (Suspicious Activity Reports)
- Banking Commission staff should be able to access and query information.
    - Search by name (Last Name/Name of Entity)
    - Search by range of dates (start date and/or end date)
    - Search by account number
    - Search by ID (CTR ID or SAR ID)
    - All searches will return tables of the following records
        - All CTRs that match the given search
        - All SARs that match the given search
    - Reports on summaries for the month and by person with subtotals and totals
    - Reports with plots of CTRs volume tendency
- Secure to external attacks since information is highly sensitive
- Field validation, a common problem is inconsistencies on naming entities
- Ability to expand to add more information than just CTRs and SARs as required in the future
- Potential for other reporting institutions to be added in the future
- Ability to delete records
- Ability to input information regarding CTRs and SARs manually for the backlog of physical reports

Appendix B.

Project Proposal

Introduction

The current way the Banking Commission collects data and conducts analysis is time intensive and leaves little room to ultimately catch and deter money launderers. The reports submitted to the Banking Commission are often inconclusive until a person's or organization's behavior is examined holistically to notice irregularities. To be able to look at the data as a whole, it would be most reasonable to have the information inputted into a database that then allows for a comprehensive analysis.

As mentioned before, with the current system, there are regular power outages and since there are desktops being used, data can be lost if changes have not been saved to documents being worked on. For that reason, we recommend a countermeasure for this sort of situation such as Uninterrupted Power Supply (UPS) or switch from desktops to laptops.

A further opportunity would be to visualize the data in a highly customizable data visualization software to automate, expedite, and increase precision in the current manual analytical process. Previously information is just kept in a Microsoft Excel Spreadsheet and analysis has just been inferred from the human eye. Larger trends from the information can be missed and a data visualization application or system from an already set up database would minimize the chance of data clean up and formatting issues.

Summary

We have explored 3 different options mapped out in the decision matrix below.

1. An encrypted email where reporting entities will send their reports and subsequently the Banking Commission will download the reports onto a locally hosted database.
2. A cloud hosted application where reporting entities upload reports to hosted application and the Banking Commission also queries and analyzes data on the cloud application.
3. A locally hosted application will be stored on a server or computer in the Banking Commission and all report submissions will be accessed through web accessible means.

The matrix below explains the pros and cons of each of the options.

Key:

Good	Neutral	Bad

	#1: File Upload w/ Local Application	#2: Cloud Hosted Application	#3: Locally Hosted Application
Cost			
Technology Infrastructure	--- (Existing computers and software can be used)	~$200-$300/year (For hosting the application and database as cloud services)	~$300-$400/year (Hardware + Software Licenses)
SSL (Sending/ Receiving information security)	--- (Online File Upload Storage provides secure transmission)	$50-$100/year (certificate of secured transmission)	$50-$100/year (certificate of secured transmission)
Domain Name	---	~$12/year (for the online application)	~$12/year (for the online application)
Security			
Data is transferred secure	Secured upload, store, and download dwith the Online File Upload Storage	Vendor provide means of security	Banking Commission staff should implement security measures for the transmission
Data is kept secure	Data is kept encrypted in local password-protected computer	Data is kept in Vendor's infrastructure. They provide physical and online security	Data is kept in local computer. Banking Commission staff must provide online security for external attacks

Data is kept confidential	Yes, can and should be encrypted	Data is encrypted on vendor's data center. Depending on vendor (i.e. google) data could not be entirely confidential	Yes, can and should be encrypted
Technological Lock-in	No	Depends of the vendor. Can have local backup	No
Maintainability			
Software	Minimal maintenance necessary, stable software. IT technician would be able to handle it	IT technician could be able to handle it, detailed training should be required	IT technician could be able to handle it, detailed training should be required
Hardware	No additional maintenance but the office computers	Maintained by provider	Server's lifespan ~3-5 years
Tier 1 Support	Banking Commission staff could likely learn	IT Technician could maybe learn	IT Technician could maybe learn
Tier 2 Support	Bank of Marshall Islands' staff	Unknown	Unknown
Scalability			
Size	Limitations of chosen Database.	You pay for what you use	Limitations of the server

Usability			
Reporting Documents	Upload flat file with raw data	Upload flat file with raw data or banks manually fill out forms in web UI	Upload flat file with raw data or banks manually fill out forms in web UI
Database Schema can be changed by the BC staff	Yes, with accurate documentation	Possibly yes, some training/expertise will be required	Possibly yes, some training/expertise will be required
Ability to backup, restore, and/or complete reinstallation	Banking Commission staff can perform it	IT Vendor will handle it	Banking Commission staff could perform it, more expertise would be required
Ramification of Internet off-island down	No new incoming reports, staff can continue working normally	System unavailable	No new incoming reports, staff can continue working normally
Data Visualization Tools	Only reports and charts	Yes	Yes
Field Validation	No. Have to be done manually	Yes	Yes
Remote Access	No	Yes	Yes
Possibility to send Law Enforcement Report	Use other tool to encrypt and decrypt it	Secured via application	Secured via application

Support for Multiple Users	Yes. Database can be shared within local network	Yes	Yes
Reasonable Response Time	Yes	Dependent on bandwidth (reasonable but sometimes unreliable)	Yes, for Banking Commission. Dependent on bandwidth (reasonable but sometimes unreliable).

Based on our research, our recommendation is to continue forward with the encrypted email and local database. We have evaluated the other alternatives and recognize that they would satisfy many of the requirements but ultimately in evaluating its sustainability this option seems like the most viable solution. In order for any of the electronic filing process to work efficiently, the employees and banks should be fully comfortable with the new filing process by the end of the summer when our support ends. Ultimately it is critical that robust Tier 1 and Tier 2 support for the solution are available in order for it to be sustainable. If there is a problem with the system that the employees may not know how to fix, there needs to be on island support. After evaluating the on island technological skill level and existing technology solutions, we recommend the option that would have the most extended support.

We have been researching into using Microsoft Access as the database management system coupled with encrypted email using Comodo digital signature. The main disadvantage to this solution is that it does not allow for remote access to the database which was one of the requests of the office for the consultants when they are abroad. Additionally, Microsoft Access does not provide the capability for automatic field validation.

Though we recommend this as the ultimate solution that we would implement, we hope this provides as a stepping stone for further solutions. As the staff in the office grows and with the recently hired IT technician, the database setup would allow for an easy exchange for a future cloud hosted application that can be maintained by the Banking Commission office.

Appendix C.

CSV File Specifications

The CTRs and SARs will be received via CSV files. A CSV file is a text file with the use of the comma as the field separator for the data.

1. Fields/columns are separated by the comma character.
2. Records/rows are terminated by newlines.
3. All records should have the same number of fields, in the same order.
4. Any field may be quoted (enclosed with double-quote characters)
   “1998”,“Jim”,”Schwartz”
5. Fields with embedded commas or double-quote characters must be quoted.
   1998,Jim,Schwartz,”Nice, friendly guy”
   1998,Jim,Schwartz,”Nice, ““friendly”” guy”
6. The first record must be a header, which contains column names for each of the fields

Required fields and format for SARs

Each row of a CSV file will correspond to a unique SAR with a unique SAR identification number. The format will be:

“Financial institution identifier”.”SAR identification number”

The SAR identification number can be whatever each respective financial institution uses to uniquely identify their SARs.

Financial institution identifiers:

Bank of Marshall Islands: 1

Bank of Guam: 2

So, if Bank of Marshall Islands has a SAR with an ID/filing number of:

SARB125478963478569

Then the CTRID would be:

1.SARB125478963478569

We used the current Banking Commission SAR format as the template for the fields and extracted a subset of the fields containing only the information needed by the Banking Commission. If a field has options, such as “yes” or “no”, the available options are listed under the numbered field as bullet points. Additionally, mandatory fields will have a “*” next to its name; all other fields are applicable if the information is available, if not, leave the field in blank.

1. SARID*
2. typeOfFinancialInstitution
3. fullNameOfFinancialInstitution*
4. EIN*
5. nameOfBranchOfficeAgency*
6. addressBranch
7. addressCityBranch
8. zipCodeBranch

9. accountNumber*
10. closedAccount*
    - Yes
    - No
11. lastNameOrNameOfEntity*
12. firstName*
13. middleName
14. gender
15. address*
16. addressCity*
17. addressState*
18. zipCode*
19. addressCountry*
20. SSNorPNorDNorEINorTIN*
21. phoneNumberResidence
22. phoneNumberWork
23. occupationOrTypeOfBusiness
24. dateOfBirth*
    - MM/DD/YYYY
25. admissionConfession*
    - Yes
    - No
26. idType* *(values are not restricted to ones specified below)*
    - Driver's License/State ID
    - Passport
    - Alien Registration
    - Other
27. idNumber*
28. idCountry*
29. relationshipToFinancialInstitution* *(can be more than one, values will be separated by commas and quoted, values are not restricted to ones specified below)*
    - Accountant
    - Agent
    - Appraiser
    - Attorney
    - Borrower
    - Broker
    - Customer
    - Director
    - Employee
    - Officer
    - Shareholder
    - Other

30. typeOfInsiderRelationship*
    - None
    - Still Employed
    - Suspended
    - Terminated
    - Resigned
31. dateOfSuspensionTerminationResignation*
    - MM/DD/YYYY
32. startDateOfSuspiciousActivity*
    - MM/DD/YYYY
33. endDateOfSuspiciousActivity*
    - MM/DD/YYYY
34. cashAmount*
35. summaryCharacterization* *(can be more than one, values will be separated by commas and quoted, values are not restricted to ones specified below)*
    - Money Laundering
    - Bribery/Gratuity
    - Check Fraud
    - Commercial Loan Fraud
    - Computer Intrusion
    - Consumer Loan Fraud
    - Counterfeit Check
    - Counterfeit Credit/Debit Card
    - Counterfeit Instrument (other)
    - Credit Card Fraud
    - Debit Card Fraud
    - Defalcation/Embezzlement
    - False Statement
    - Misuse of Position or Self Dealing
    - Mortgage Loan Fraud
    - Mysterious Disappearance
    - Wire Transfer Fraud
    - Other
36. affectedFinancialInstitution*
    - Yes
    - No
37. lastNameOrEntityNameForAssistance
38. firstNameForAssistance
39. tittleOccupation
40. phoneNumber
41. datePrepared*
    - MM/DD/YYYY
42. narrative*

Required fields and format for CTRs

The CTRs will be broken up into two CSV files. One file will have information for the Person(s) involved in transactions (PIT_info) and another file will have the rest of the information for the CTRs (CTR_info). Additionally, mandatory fields will have a "*" next to its name; all other fields are applicable if the information is available, if not, leave the field in blank.

PIT_info:
Each row will correspond to a unique "Person Involved in Transaction" entry for each CTR that has been filed. This information comes from the current CTR format that each bank files, Banking Commission/FinCen format: Part I Person Involved in Transaction. For example, if there are three CTRs filed in a given time period: CTR1, CTR2, CTR3. Where CTR1 and CTR2 have 3 persons involved in the transaction and CTR3 has 1 person involved in the transaction. Then, PIT_info will have a total of 7 entries, with each row corresponding to one person involved in the transaction across all of the CTRs.

CTR_info:
Each row will correspond to a unique CTR. The fields in each entry were derived from Part II and Part III of the current CTR format that each bank files with the Banking Commission/FinCen. PIT_info and CTR_info will be linked together through a CTRID.
Each "person involved in transaction" entry will have the CTRID of the CTR that they are associated with. In order to ensure that CTRID is unique across the two financial institutions we require that each financial institution include a unique identifier as part of the CTRID. The format will be:

"Financial institution identifier"."CTR identification number"

Using the same format specified in the SAR CSV section and the same financial institution identifiers:

Bank of Marshall Islands: 1
Bank of Guam: 2

If Bank of Guam has a CTR with an ID/filing number of:

CTRB1633102000001

Then the CTRID would be:

2.CTRB1633102000001

Fields for PIT_info:

1. CTRID*
2. relationshipToTransaction*
   - Person on whose behalf transaction was conducted
   - Person conducting transaction for another
   - Person conducting transaction on own behalf
   - Courier Service (private)

3. lastNameOrNameOfEntity* *(for the case of Part I, Section A, Item 5. If the person is 'Doing Business As' a particular company, the value of this field should be as follows: "Matias Rosales, Company A". This means Matias Rosales doing business as Company A)*
4. firstName*
5. middleName
6. gender
7. occupationOrTypeOfBusiness
8. SSNorEIN*
9. address*
10. addressCity*
11. addressState*
12. zipCode*
13. addressCountry*
14. dateOfBirth*
    MM/DD/YYYY
15. contactPhoneNumber
16. emailAddress
17. idType**(values are not restricted to ones specified below)*
    Driver's License/State ID
    Passport
    Alien Registration
    Other
18. idNumber*
19. idCountry*

Fields for CTR_info:

1. CTRID*
2. dateOfTransaction*
    MM/DD/YYYY
3. cashDirection* *(value can be other than the ones specified below)*
    Withdrawal
    Deposit
    Wire Deposit
    Wire Withdrawal
    Currency Exchanged
    Foreign Currency
    Negotiable Instruments Purchased
    Negotiable Instruments Cashed
    Other
4. cashAmount* *(in case of multiple deposits/withdrawals, put the aggregated value)*
5. accountNumbers* *(can be more than one, values will be separated by commas and quoted)*
6. typeOfFinancialInstitution

7. fullNameOfFinancialInstitution*
8. nameOfBranchOfficeAgency*

Reference Files
ctrs.csv
sars.csv
pit.csv

Appendix D.

Tables Diagram

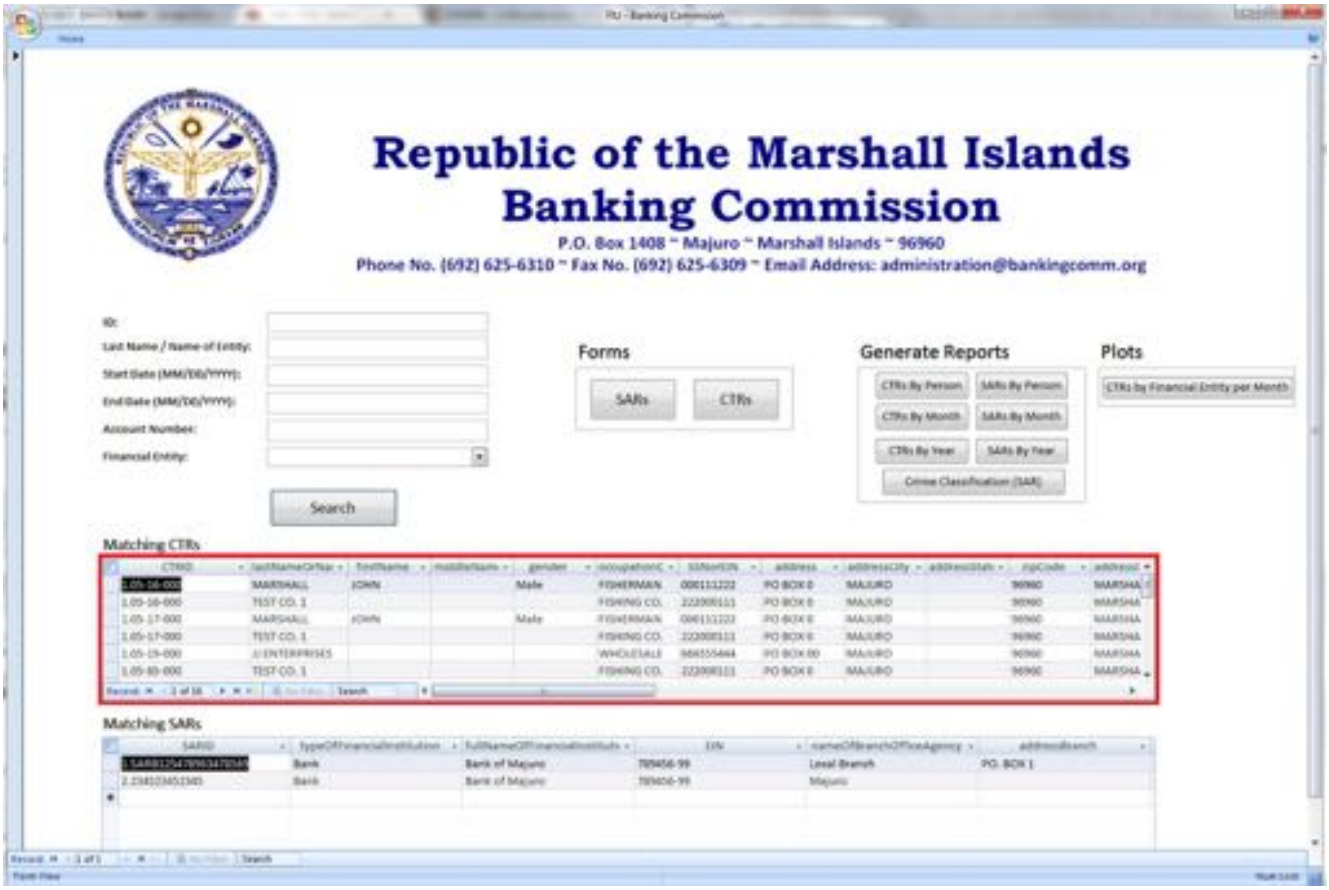
Appendix E.

How to use the Forms

MainForm:

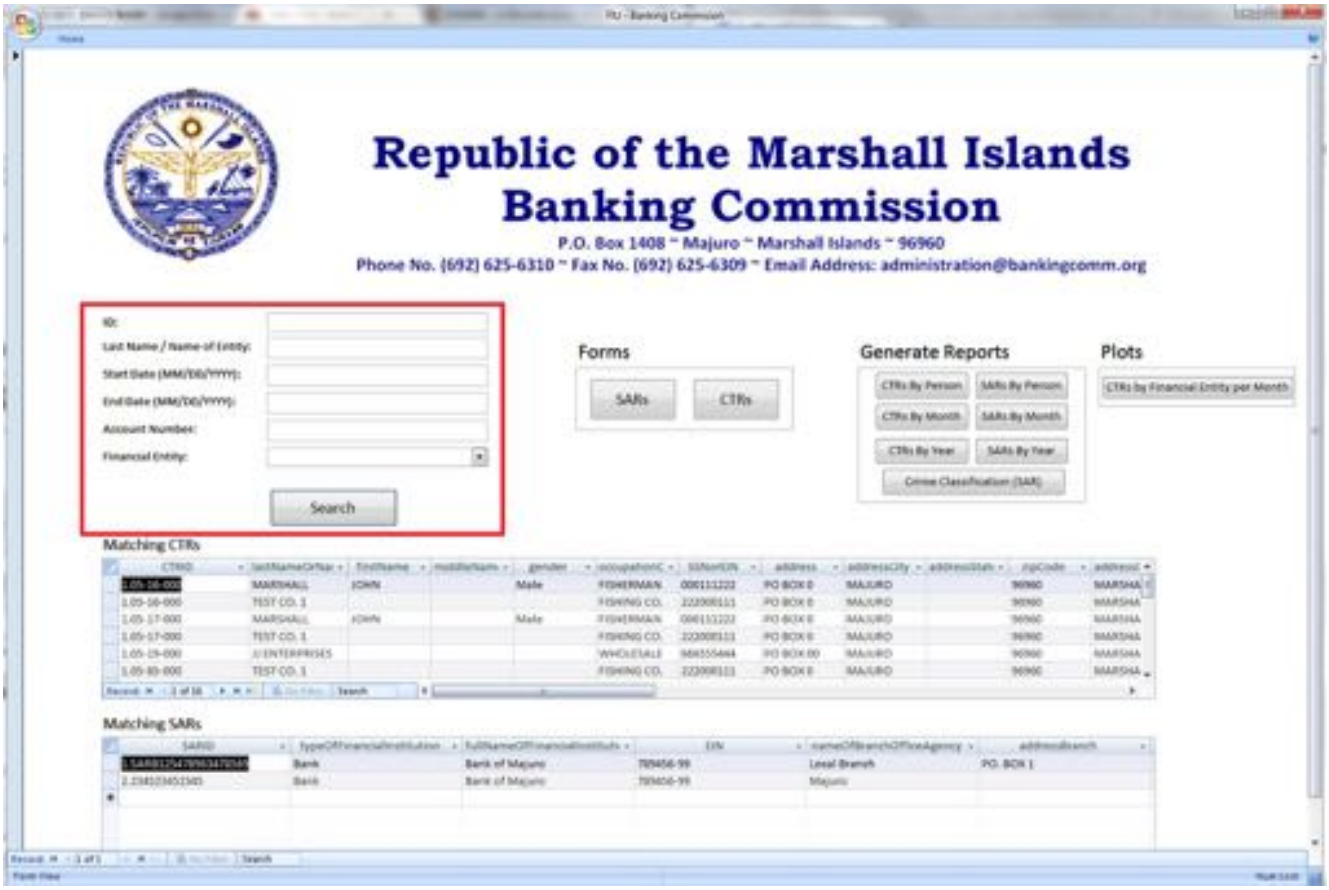
- The **MainForm** is the home page for the application

- The CTRs **SearchQuery subform** displays matching CTRs from the **SearchQuery**



- The **SearchQuerySARs** subform displays matching SARs from the **SearchQuery**

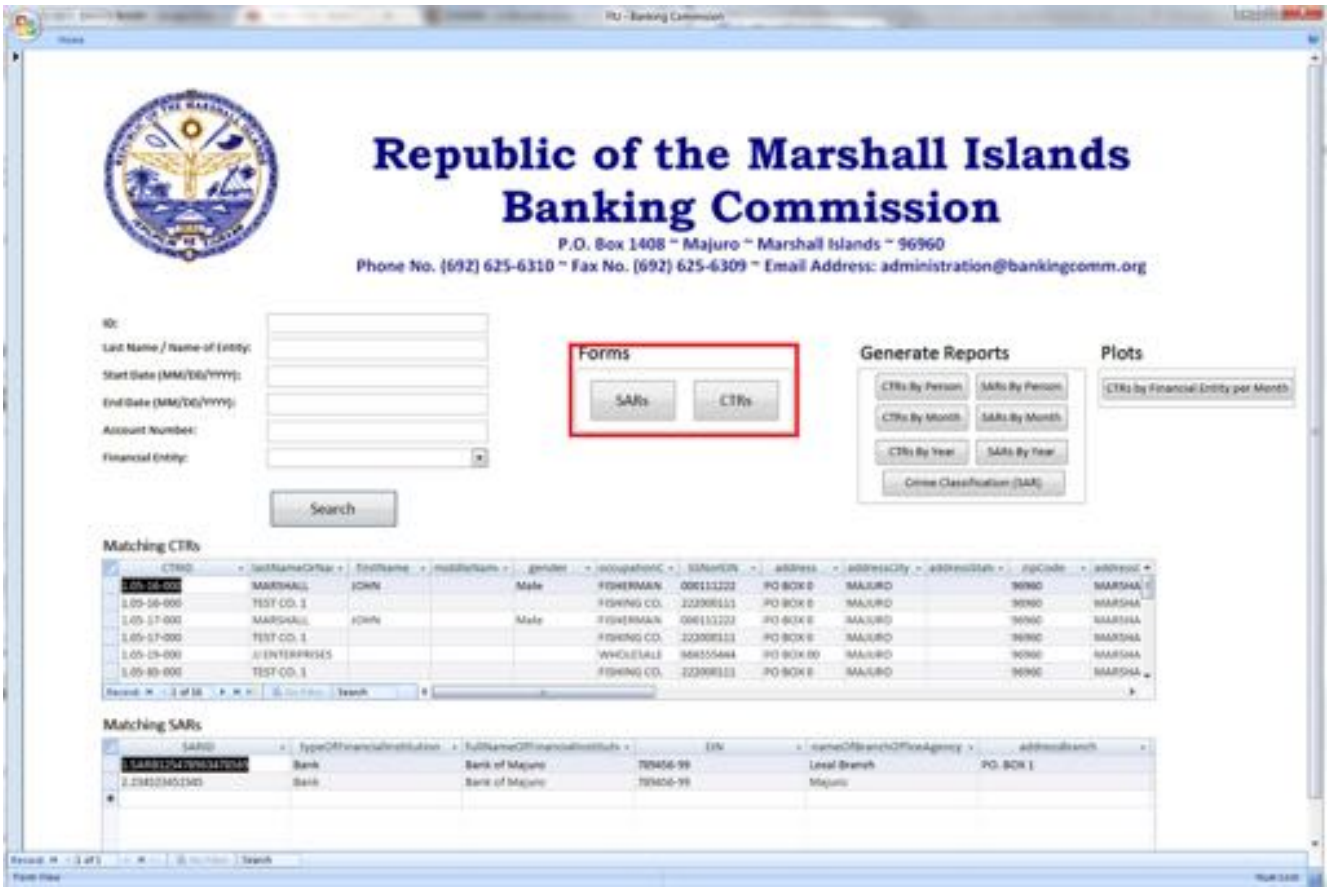
- You can search by **ID**, **Last Name / Name of Entity**, between a **Start Date** and an **End Date**, **Account Number**, or **Financial Entity**.
- When you click on **Search**, it runs **SearchQuery**. The matching results are displayed in the two subforms discussed prior.



- There are reports that generate aggregated results by **Person**, **Month**, **Year** and **Type of Crime** for SARs.

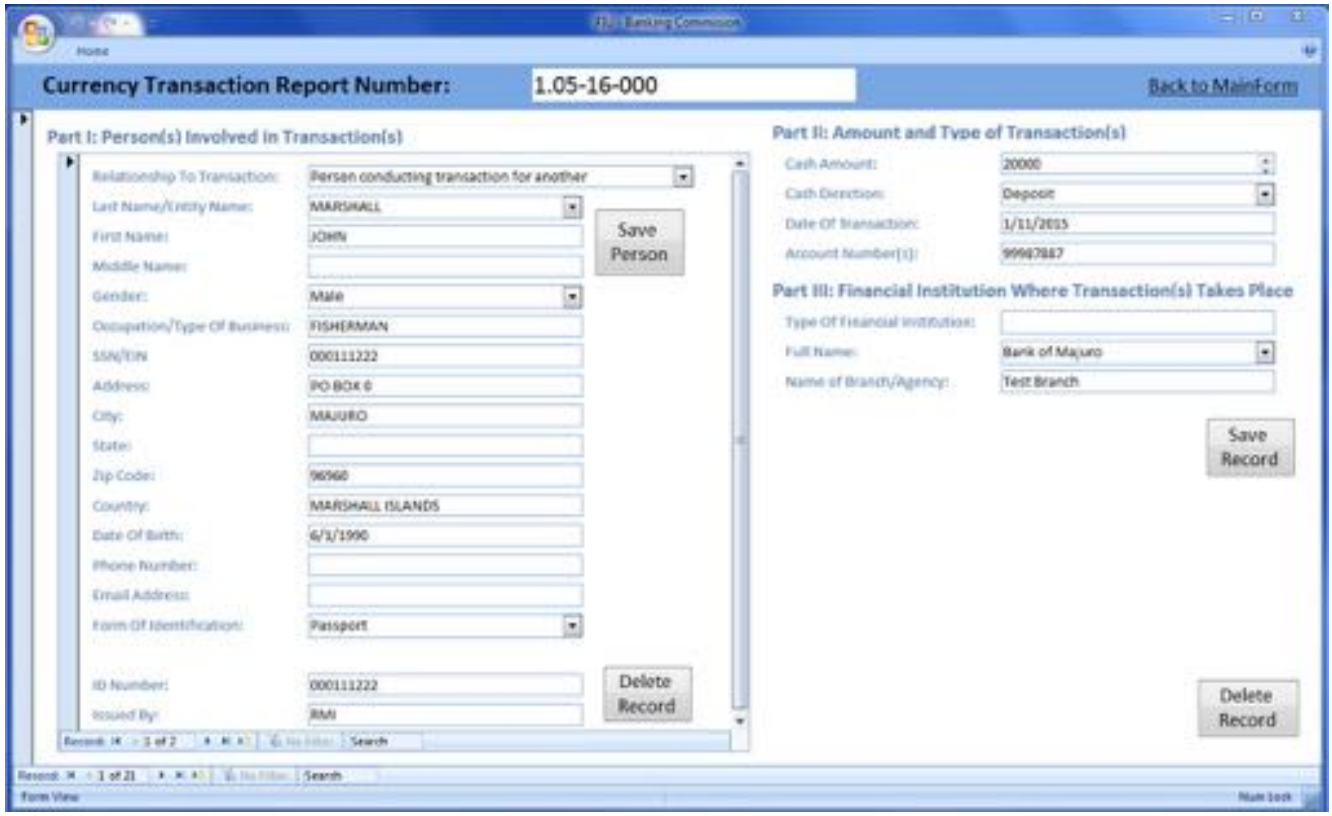
- There is a plot that generates a trendline of **Amount of CTRs** over time, aggregated by months, for every **Financial Entity**.

- To view/edit/add individual CTRs and SARs.

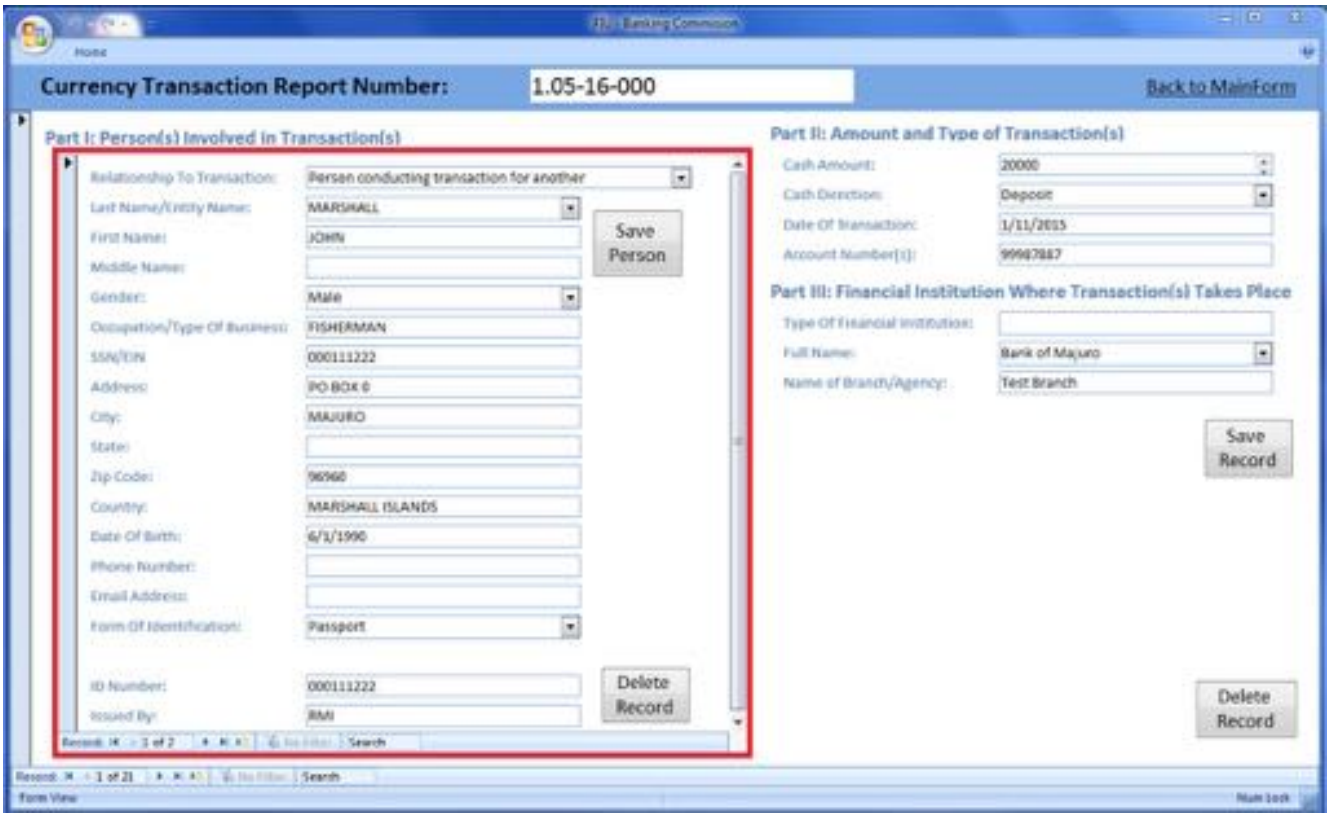


CTRs:

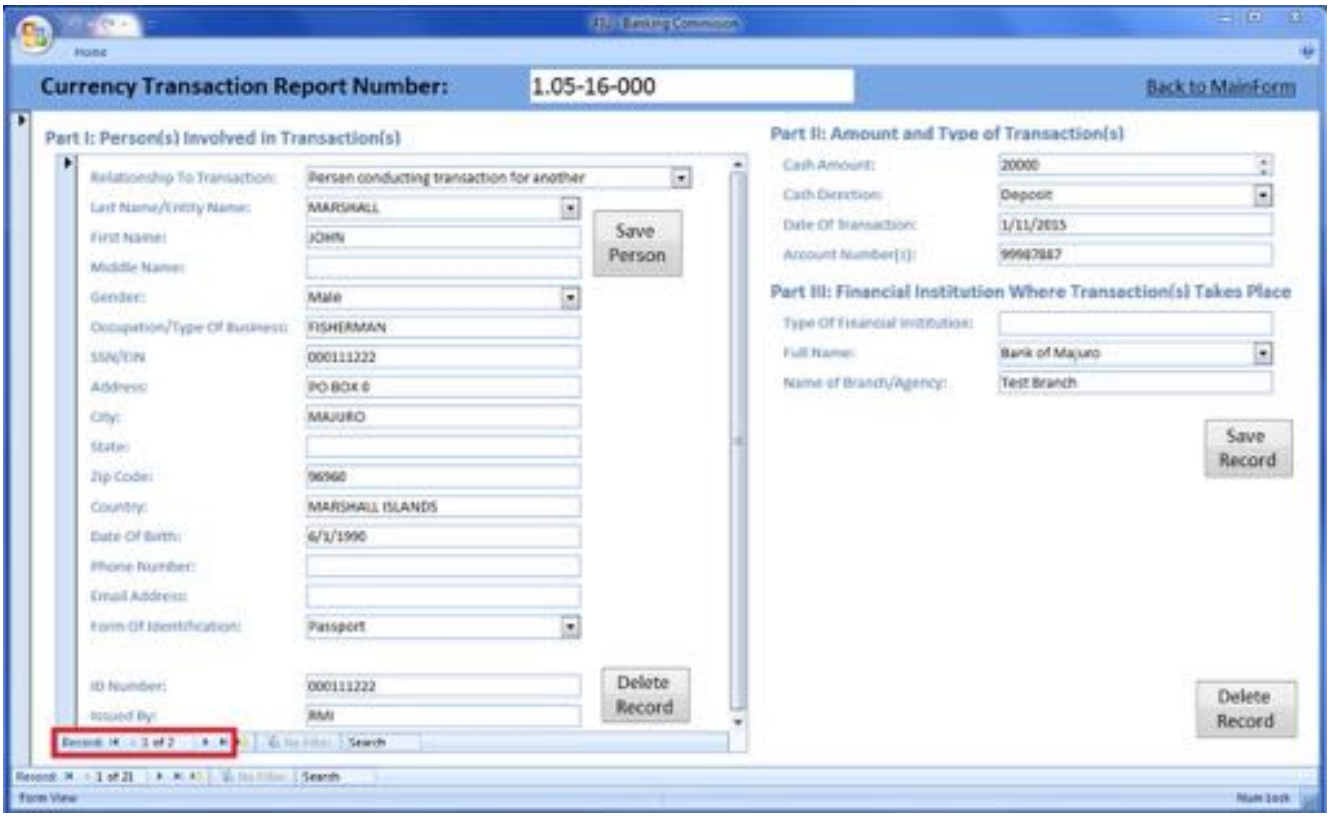
- The CTRs form is where you can view, edit, and add CTRs.



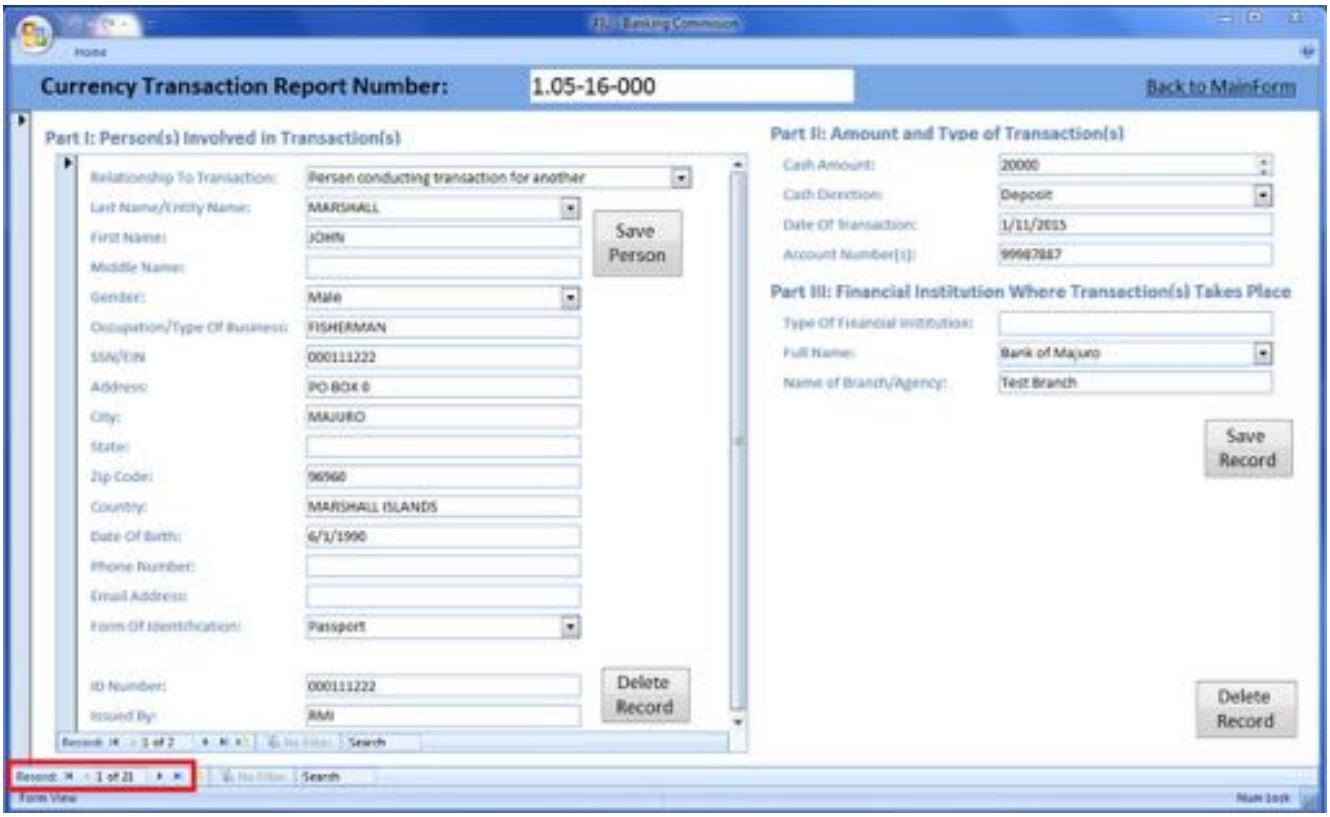
- Person(s) involved in Transaction(s) within CTRs are displayed in Part I.



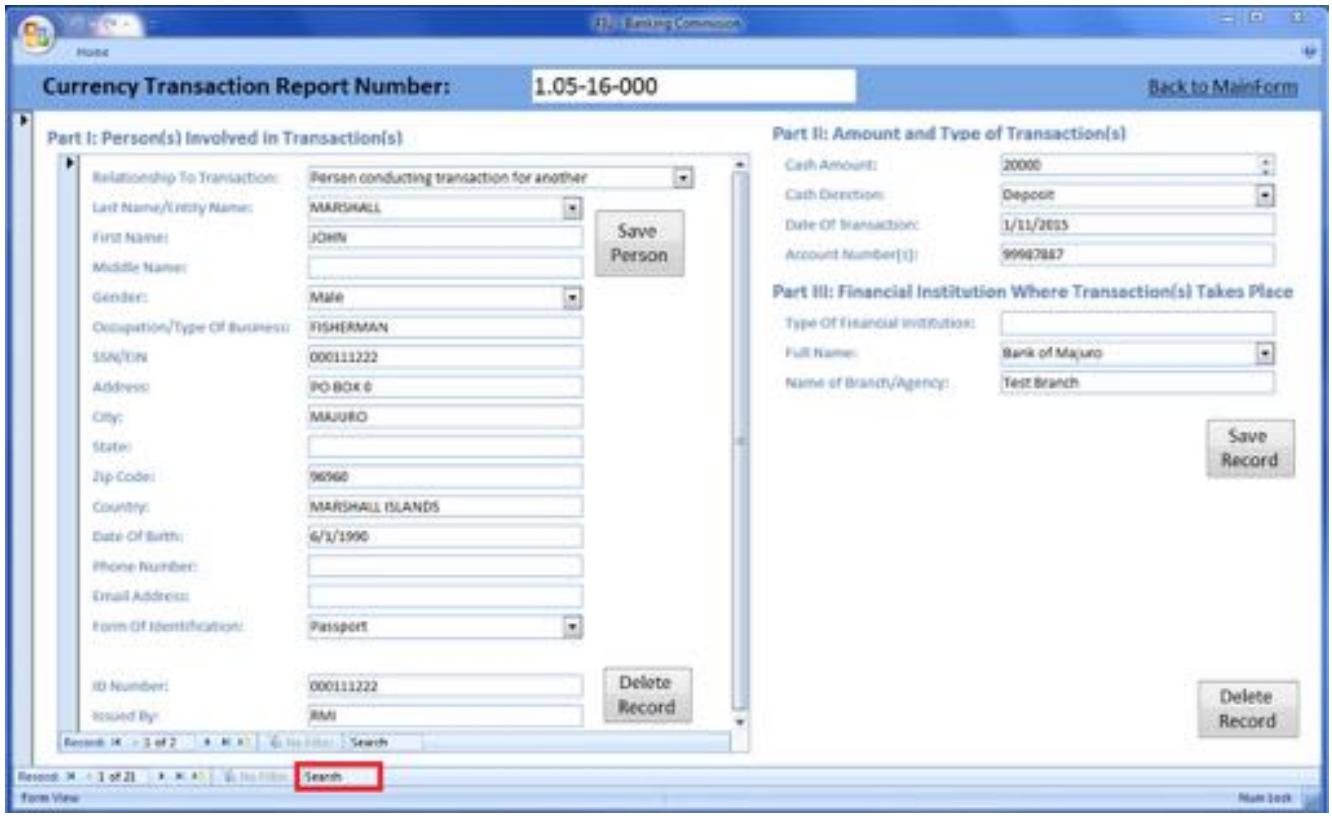
- You can scroll through Person(s) Involved in Transaction in the current CTR



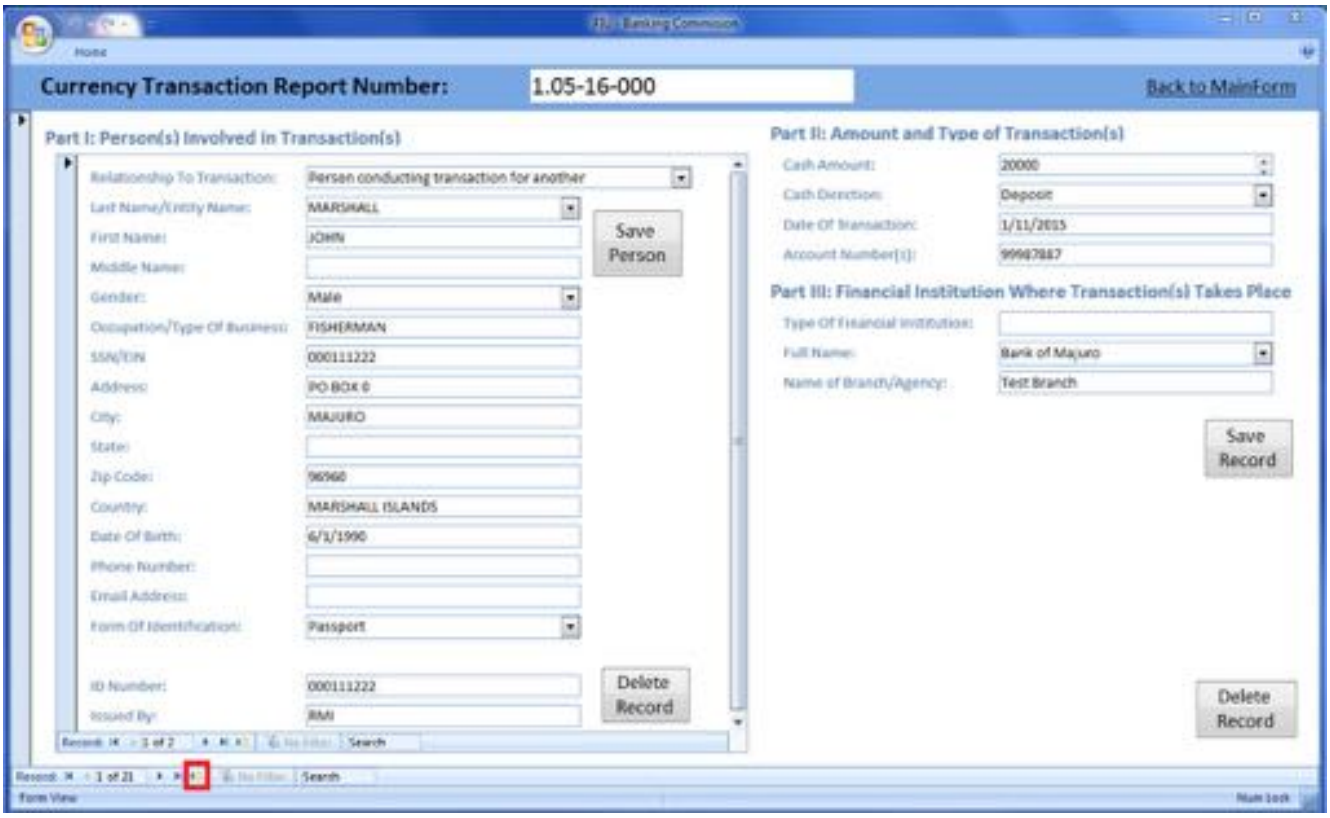
- You can scroll through CTRs records



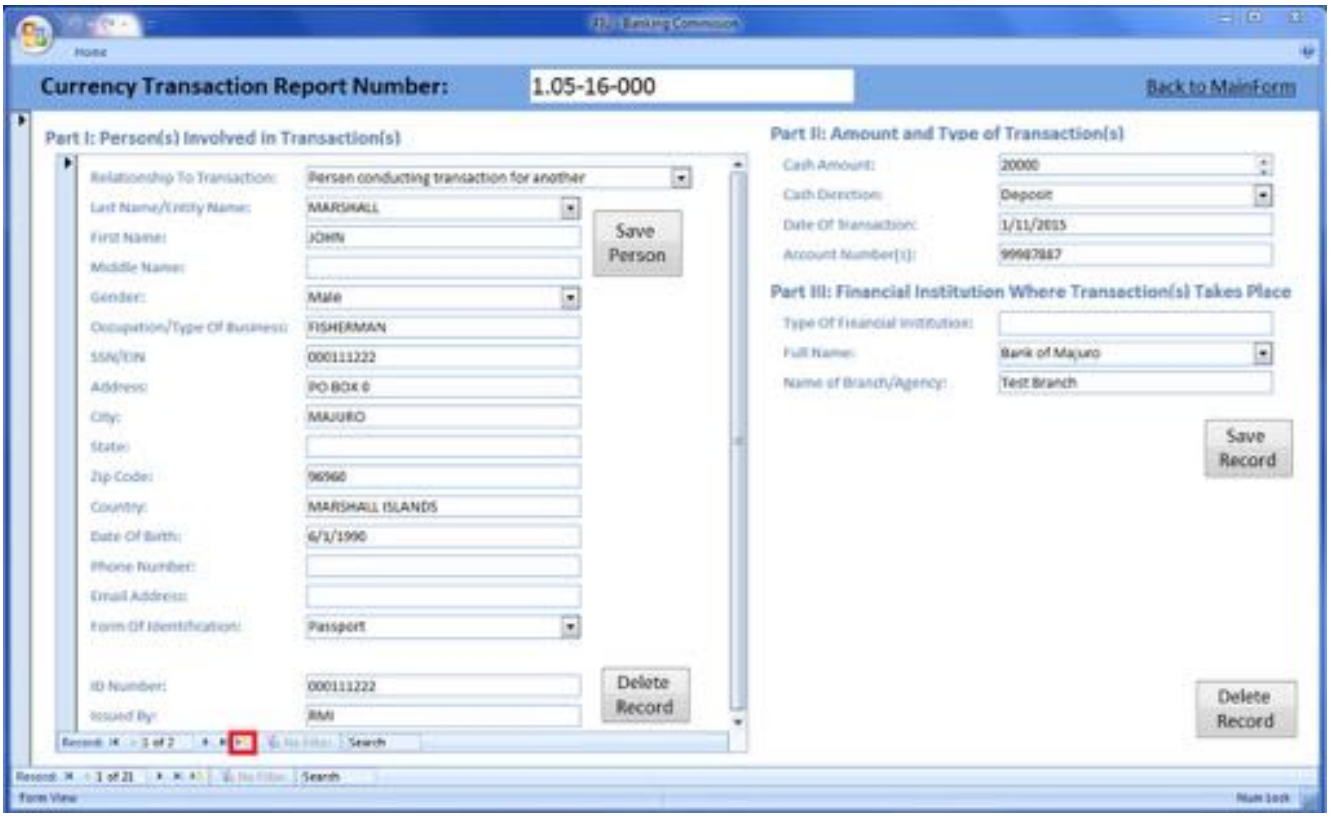
- You can search for a CTR by **CTRID**



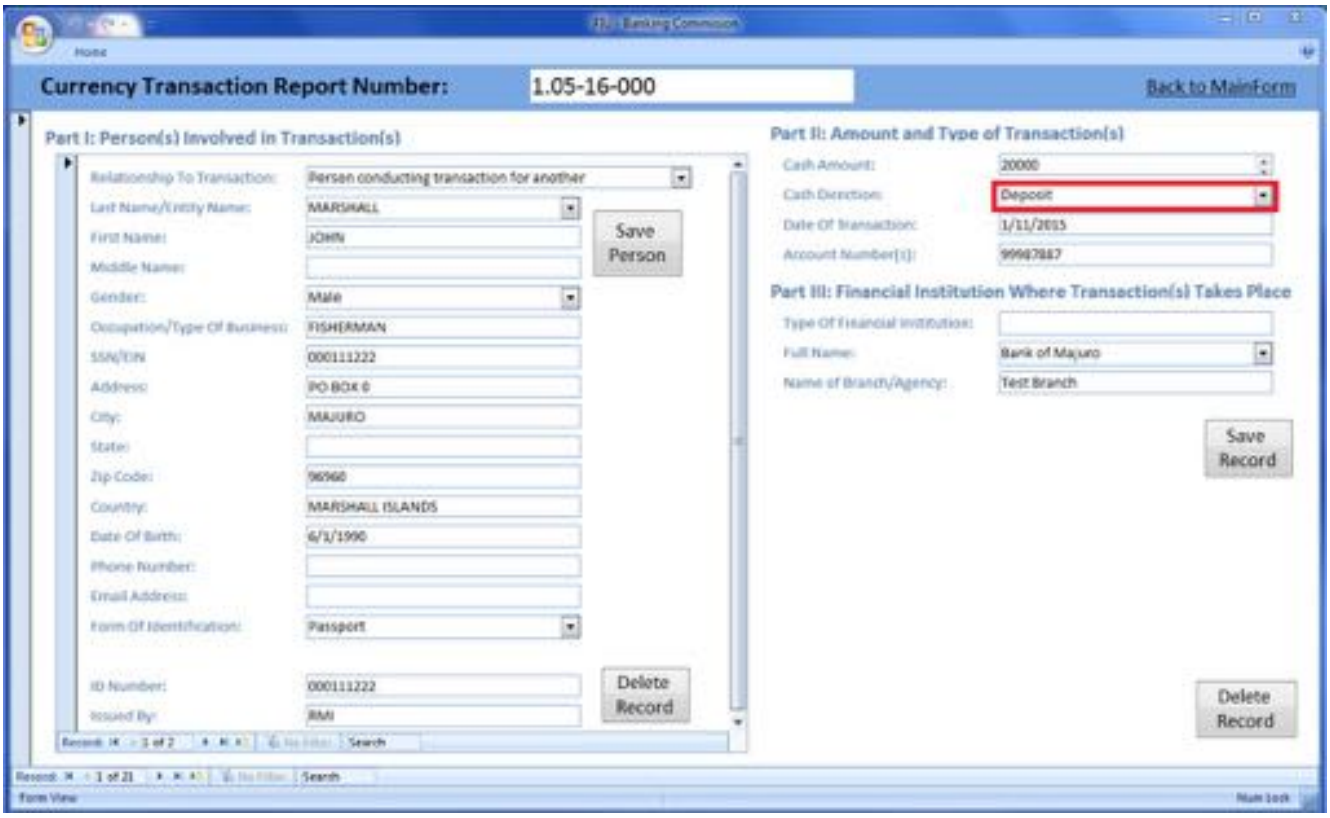
- To add a new CTR, click on the arrow pointing right with the yellow *
- Note: You **MUST** enter the CTRID **BEFORE** filling out any other fields

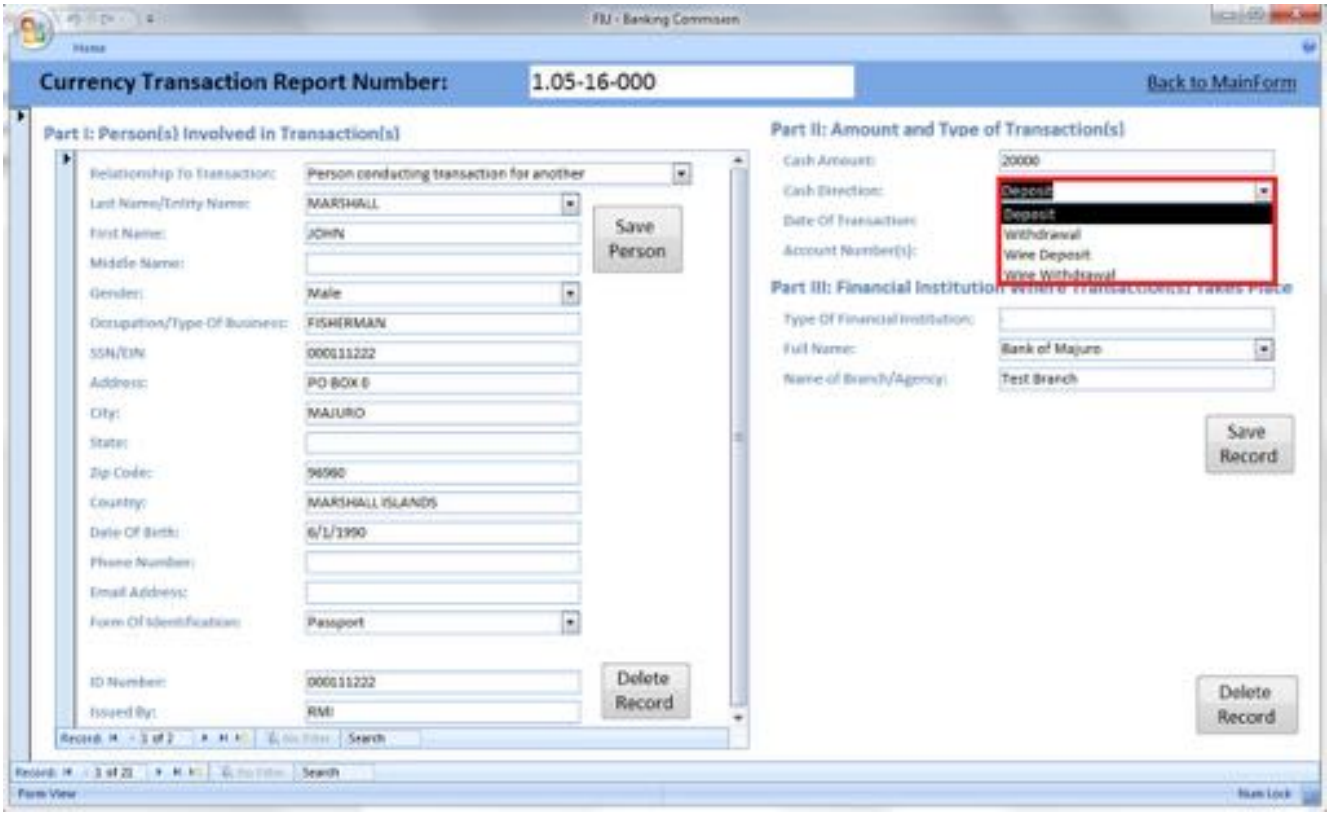


- To add a new person to a CTR, click on the arrow pointing right with the yellow *

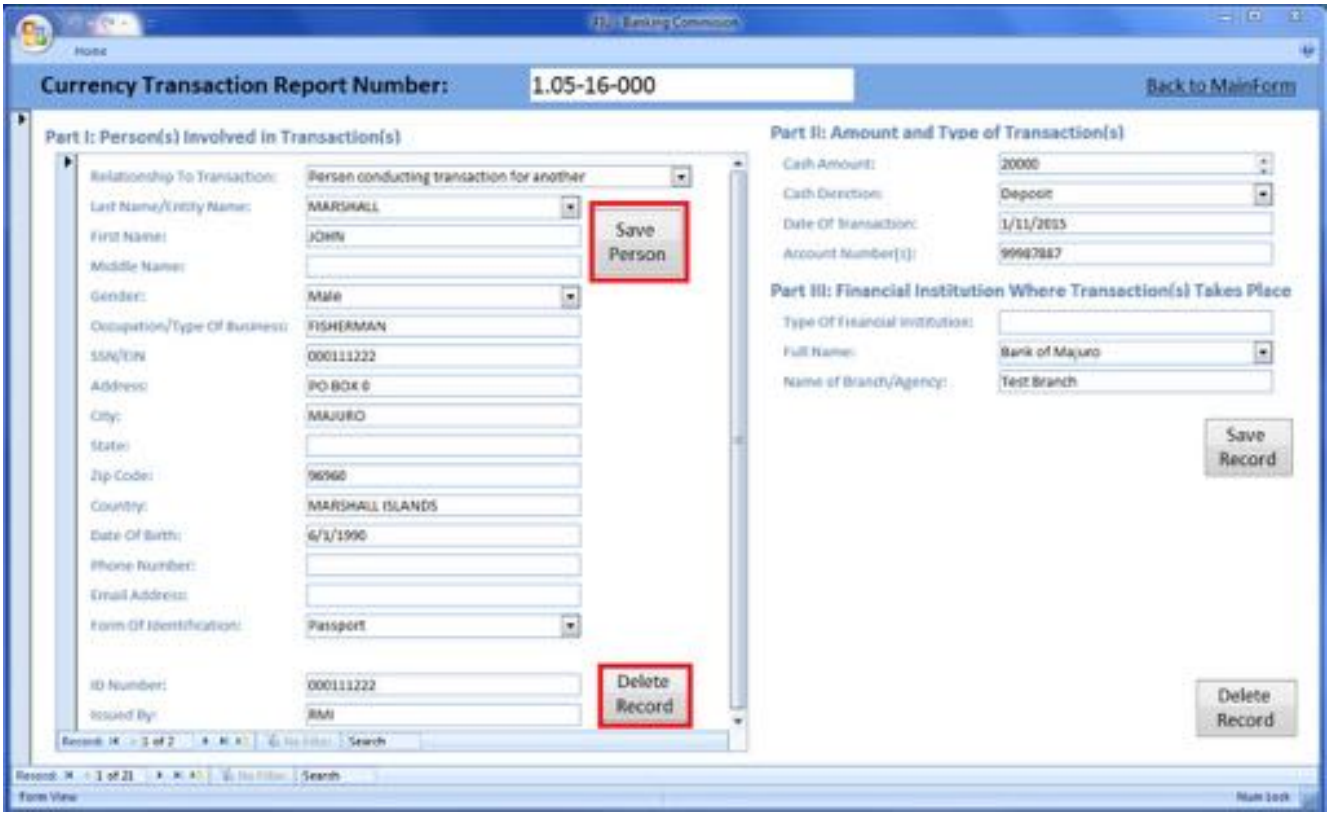


- Fields with an arrow in the text box have values that can be selected

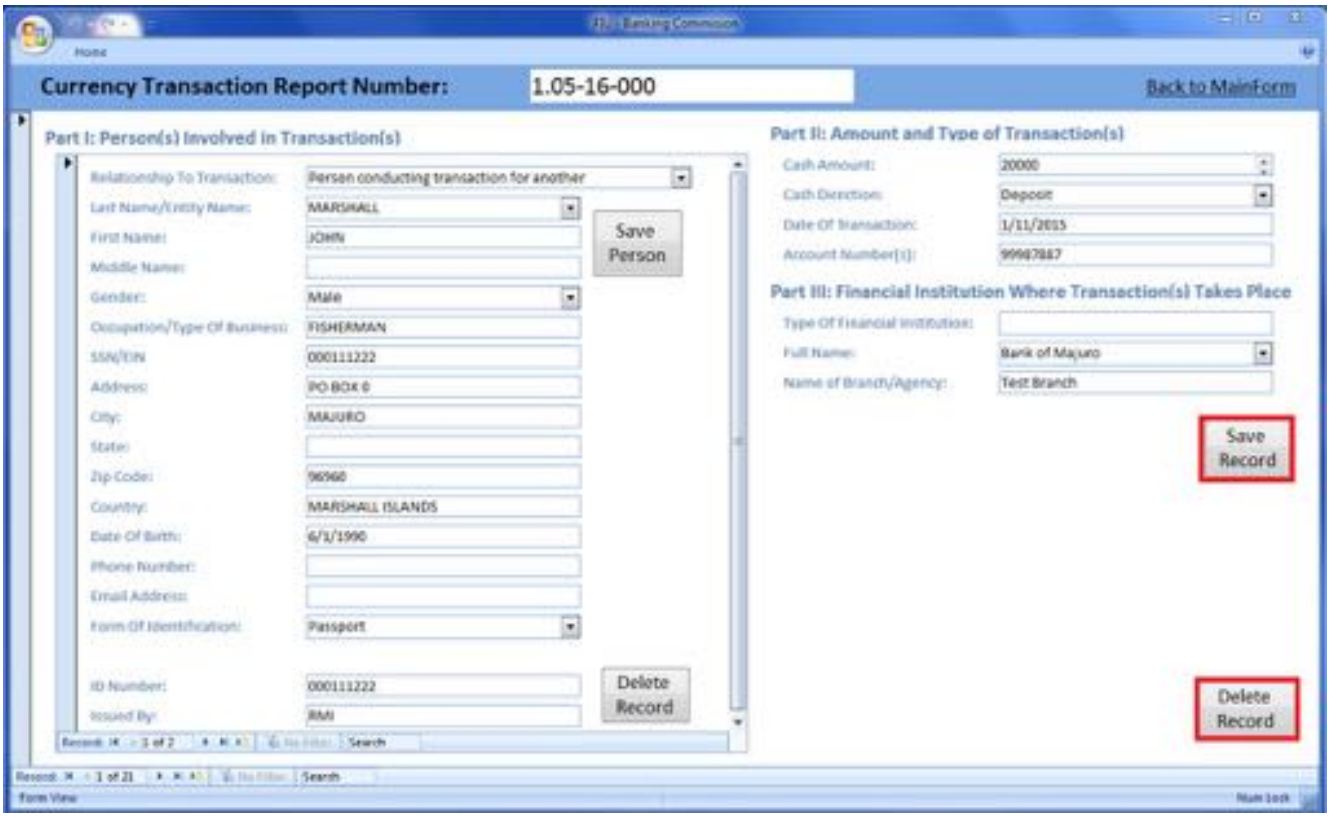



FIU - Banking Commissen
Currency Transaction Report Number:
1.05-16-000
Back to MainForm
Part I: Person(s) Involved in Transaction(s)
Relationship To Transaction:
Person conducting transaction for another
Last Name/Entity Name:
MARSHALL
First Name:
JOHN
Middle Name:
Gender:
Male
Occupation/Type Of Business:
FISHERMAN
SSN/EIN
000111222
Address:
PO BOX 0
City:
MAJURO
State:
Zip Code:
96960
Country:
MARSHALL ISLANDS
Date Of Birth:
6/1/1990
Phone Number:
Email Address:
Form Of Identification:
Passport
ID Number:
000111222
Issued By:
RMI
Save Person
Delete Record
Part II: Amount and Type of Transaction(s)
Cash Amount:
20000
Cash Direction:
Deposit
Deposit
Withdrawal
Wire Deposit
Wire Withdrawal
Date Of Transaction:
Account Number(s):
Part III: Financial Institution
Type Of Financial Institution:
Full Name:
Bank of Majuro
Name of Branch/Agency:
Test Branch
Save Record
Delete Record
Search
Form View
Num Lock

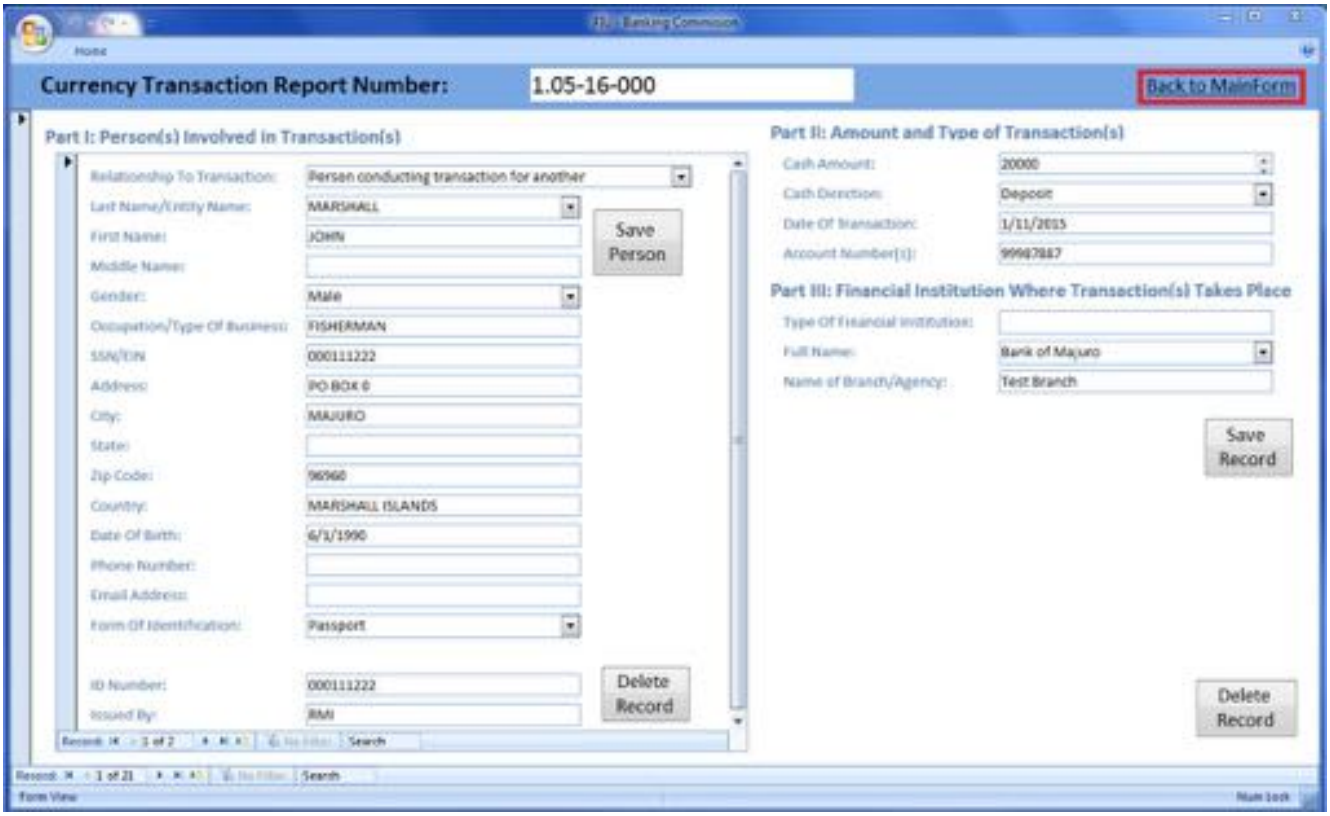
- To **Save** or **Delete** a Person(s) Involved In Transaction(s), click the respective buttons



- To **Save** or **Delete** a CTR, click the respective buttons
- Note: Always **Save** the Person(s) Involved In Transaction(s) before filling out the rest (Part II and III), as a best practice.

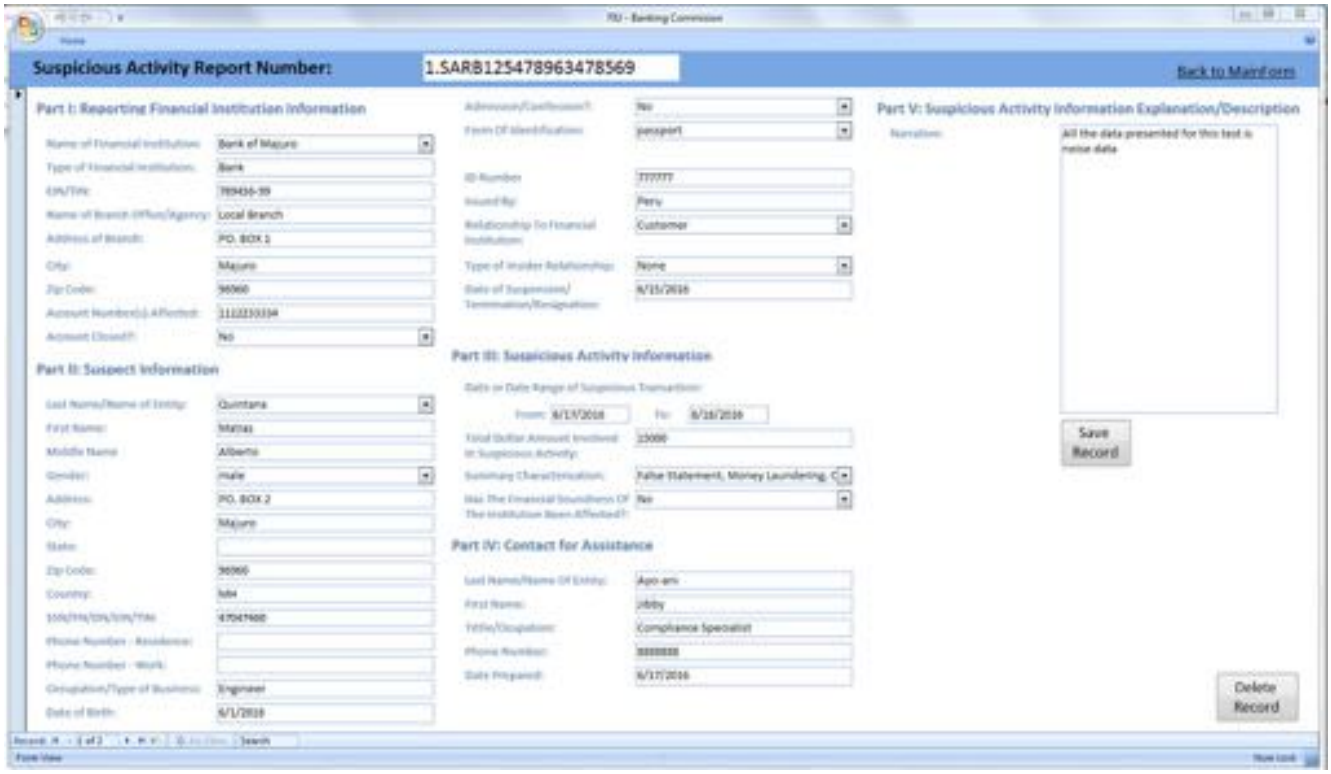


- To go back to the **MainForm**

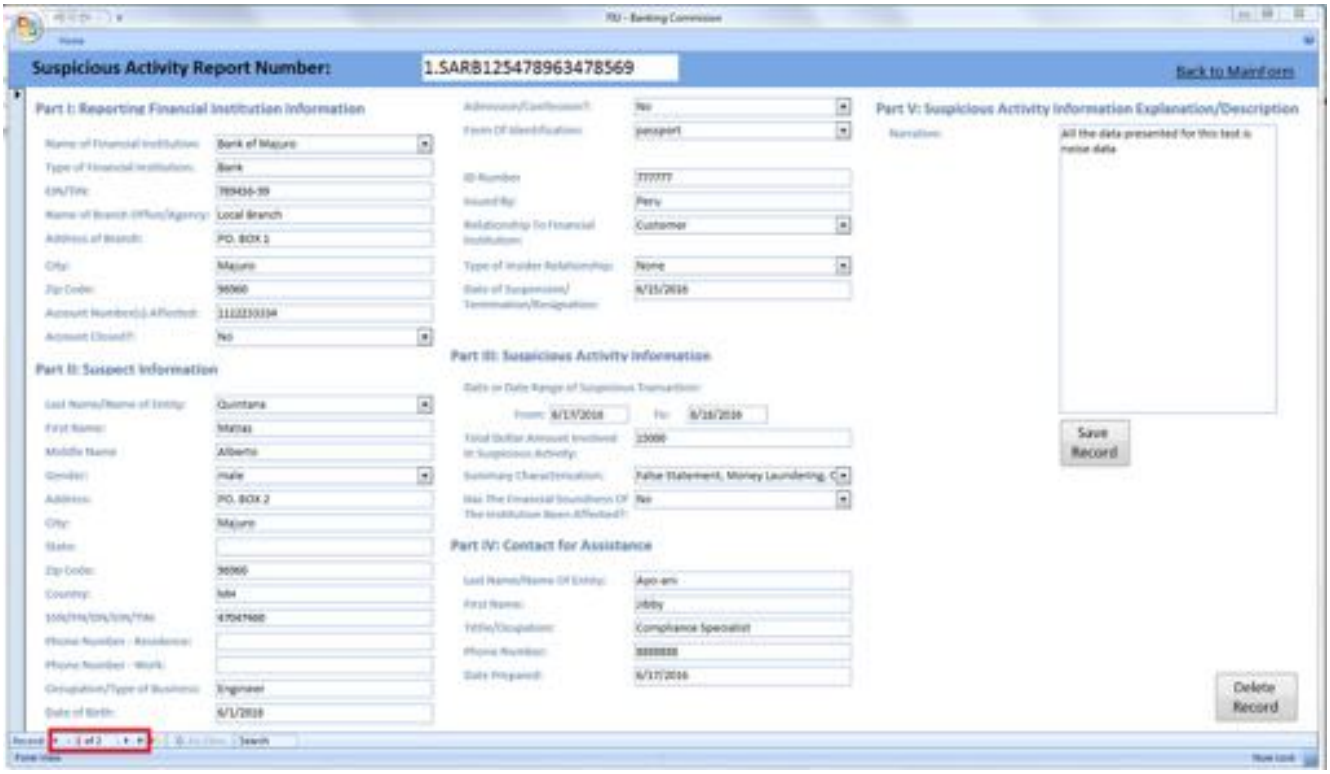


SARs:

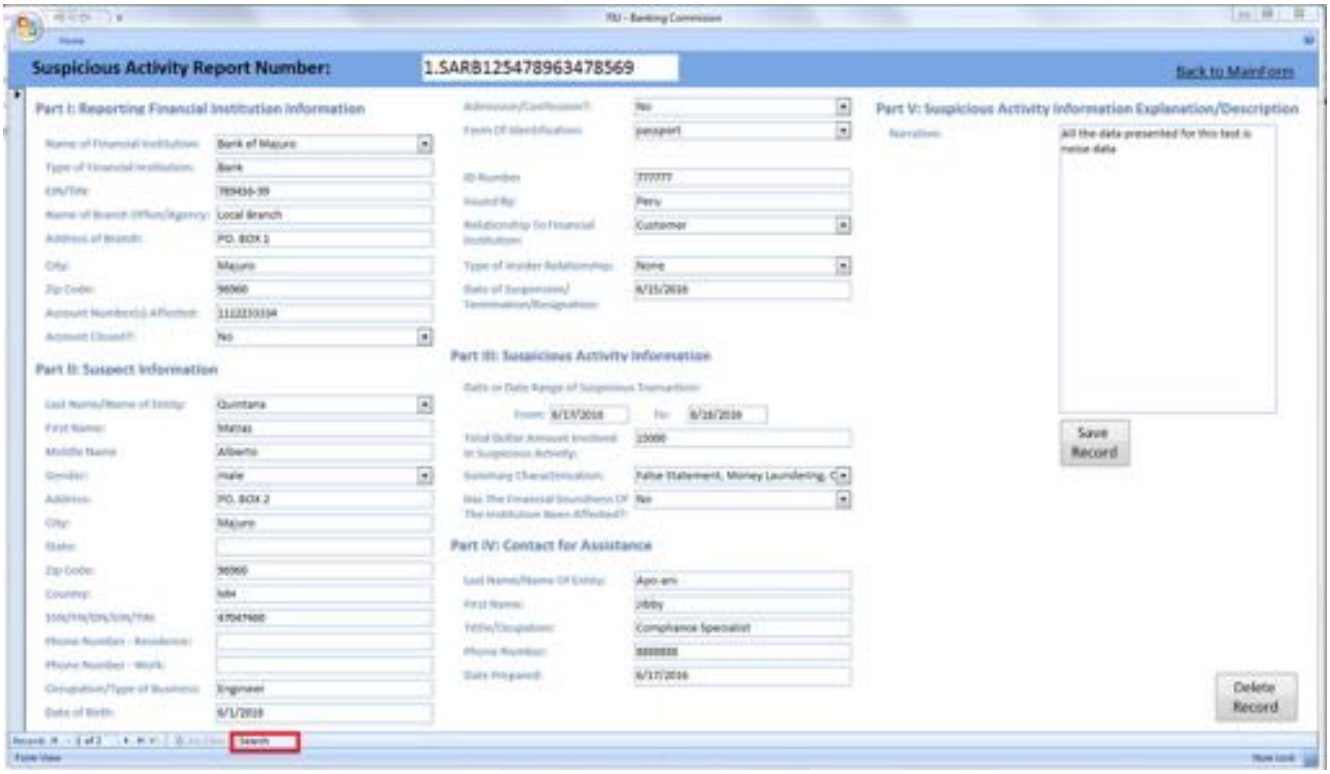
- To **SARs** form is where you can view, edit and add **SARs**



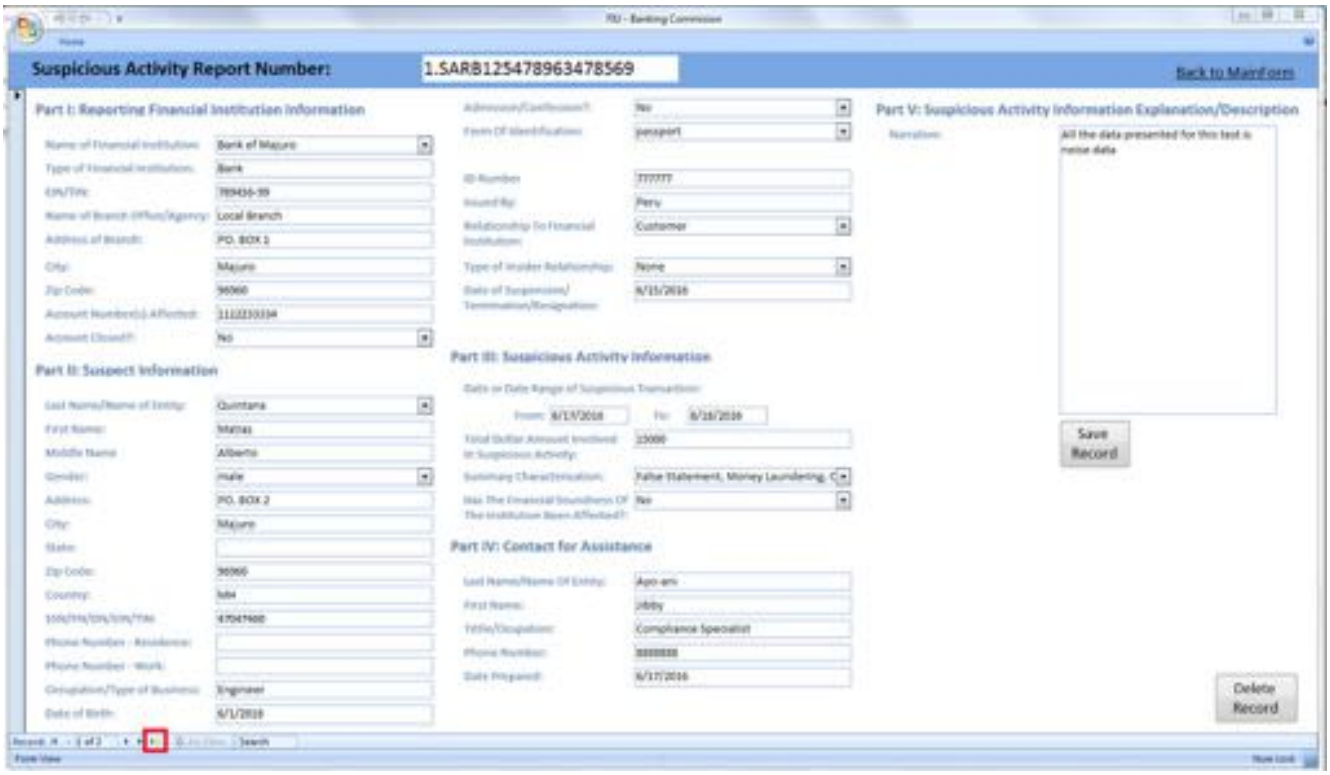
- You can scroll through the SAR entries



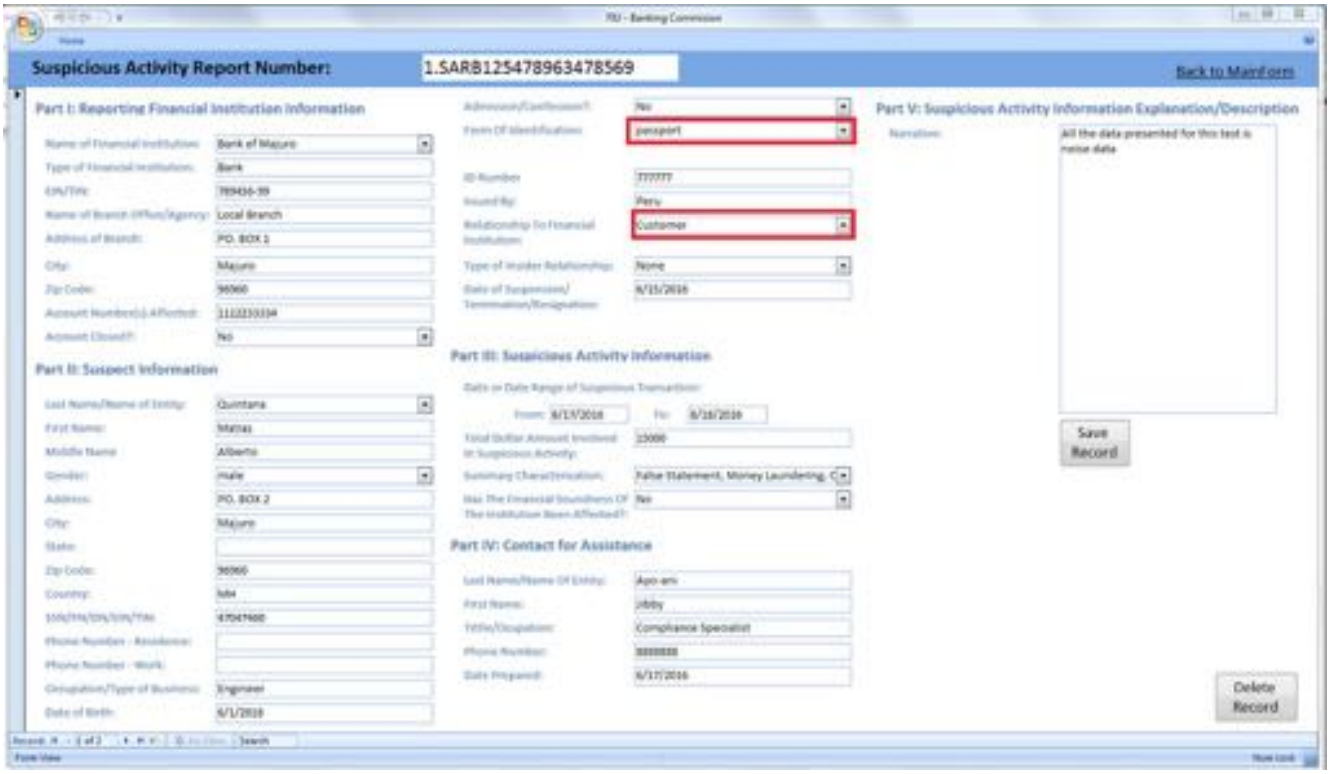
- You can search for a SAR by **SARID**



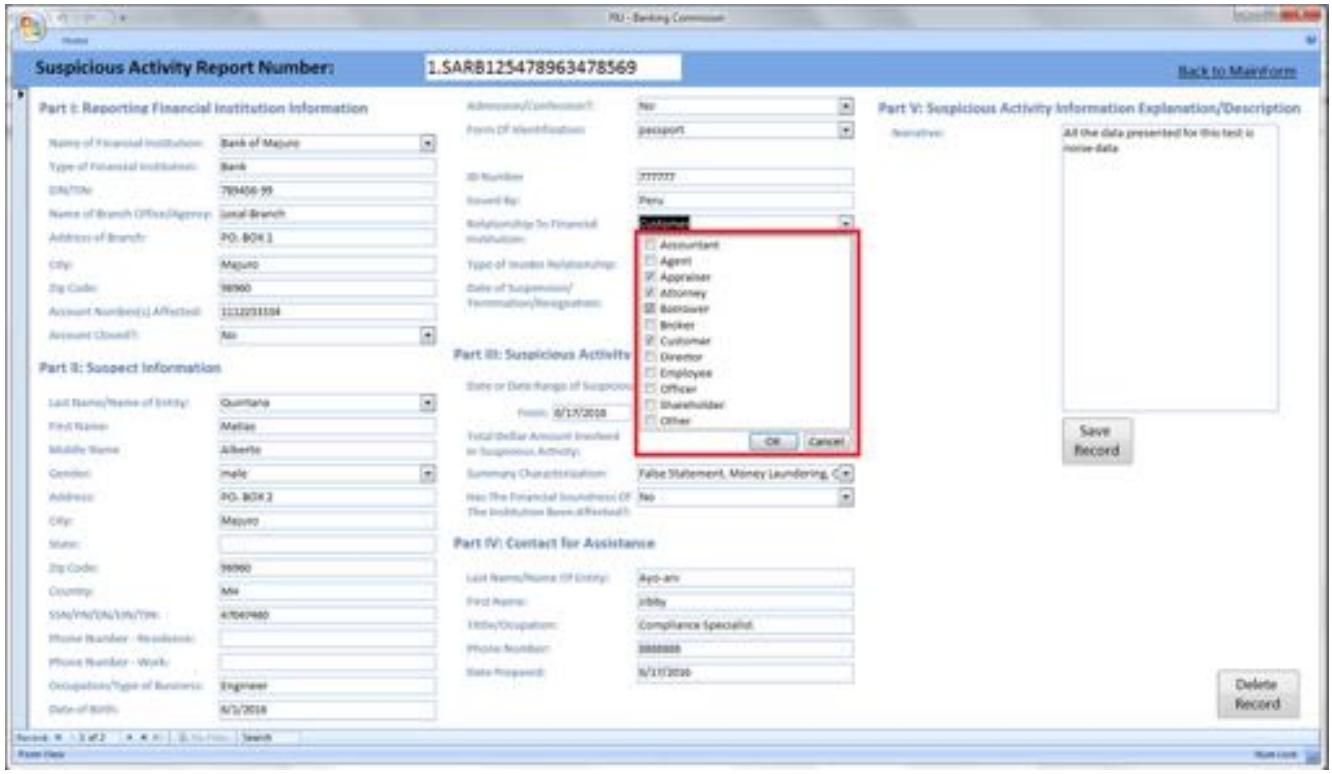
- To add a new SAR, click on the arrow pointing right with the yellow *
- Note: You **MUST** enter the SARID **BEFORE** filling out any other fields



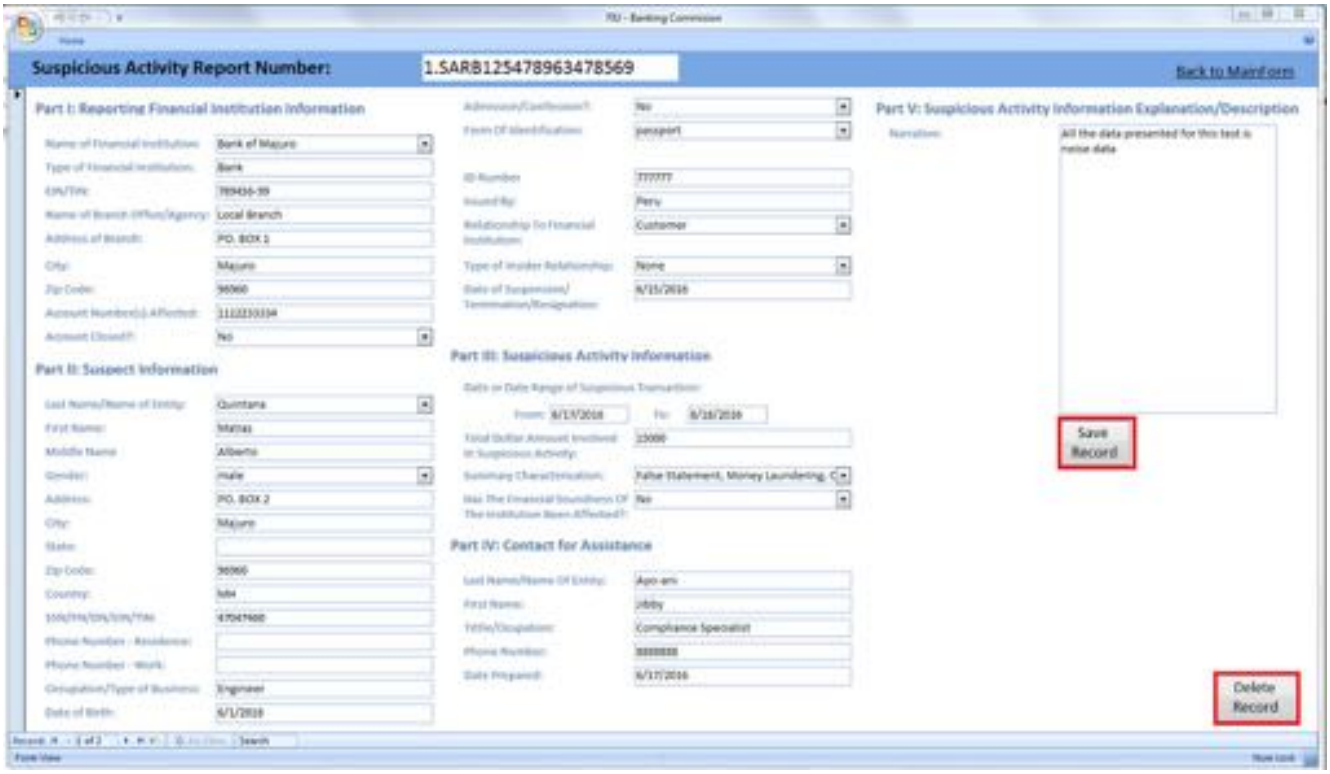
- Fields with an arrow in the text box have values that can be selected



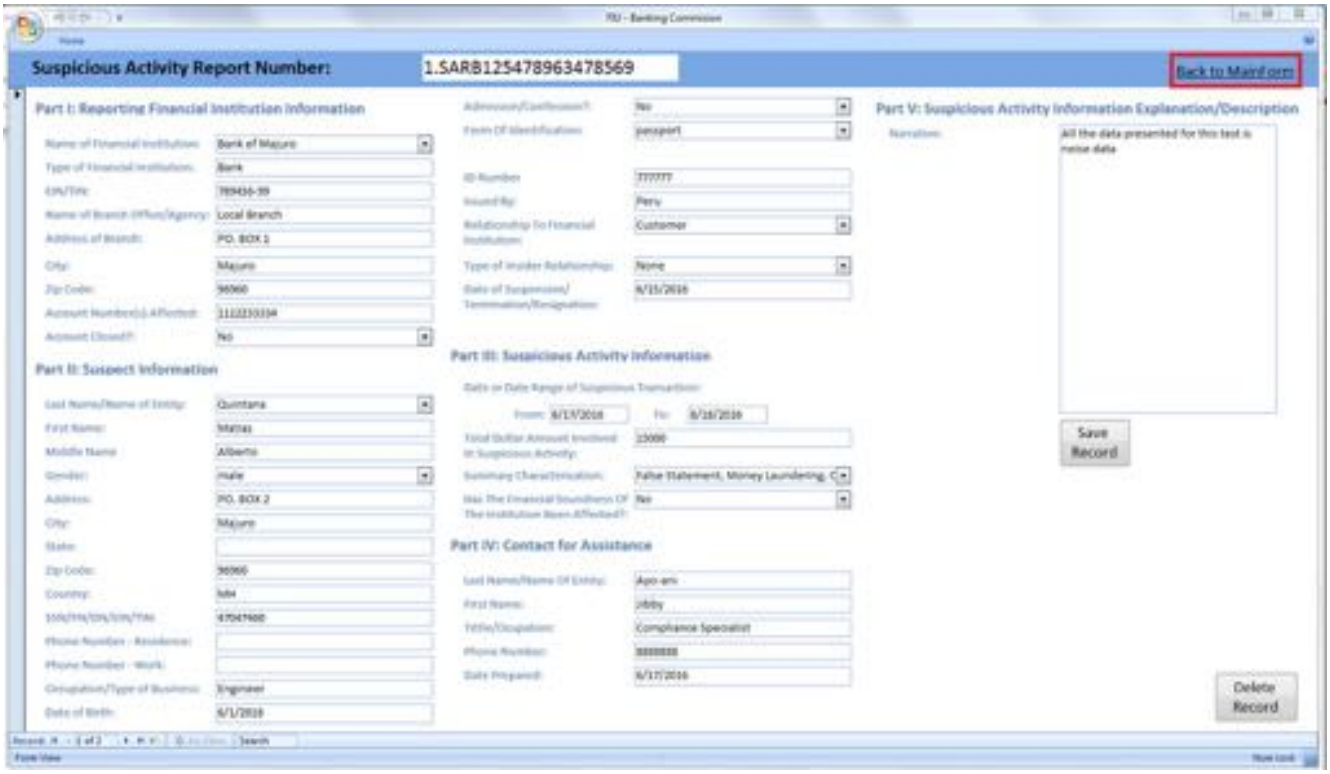
- Some of them allow for more than one option to be selected.



- To **Save** or **Delete** an SAR, click the respective buttons



- To go back to the **MainForm**



Appendix F.

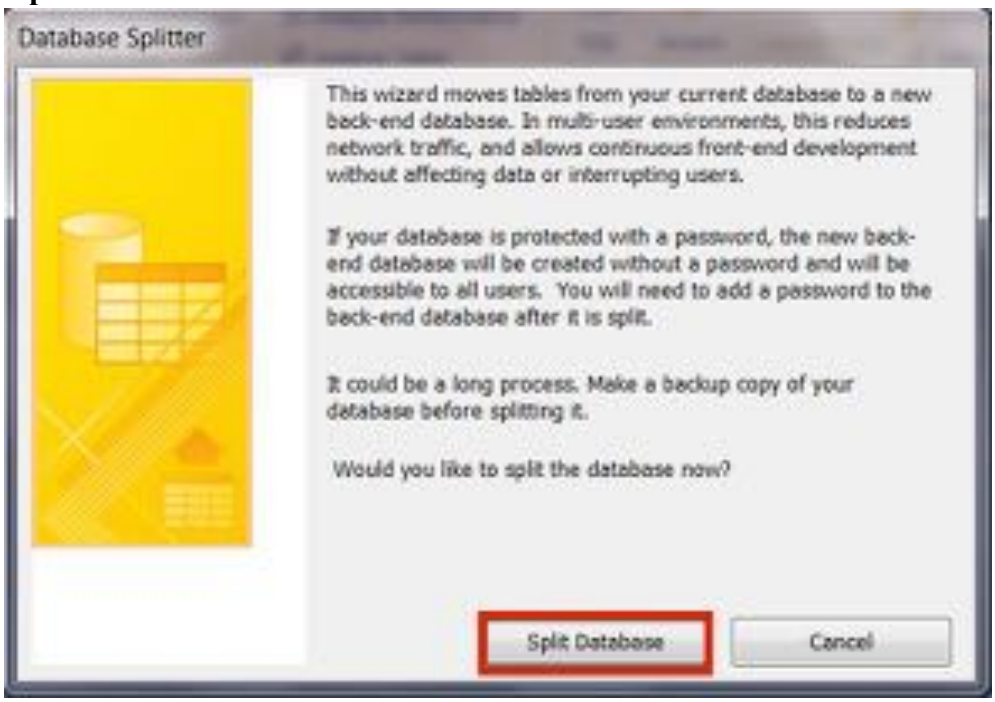
Splitting an Access database:

In order to allow multiple users to use the database concurrently, it is necessary to split the Microsoft Access database. When you split a database, you reorganize it into two files: a back-end database that contains the data tables and a front-end database that contains queries, reports, and forms. Each user has a local copy of the front-end database and then one user has the back-end database. The other users can access that copy of the back-end database over the local network.

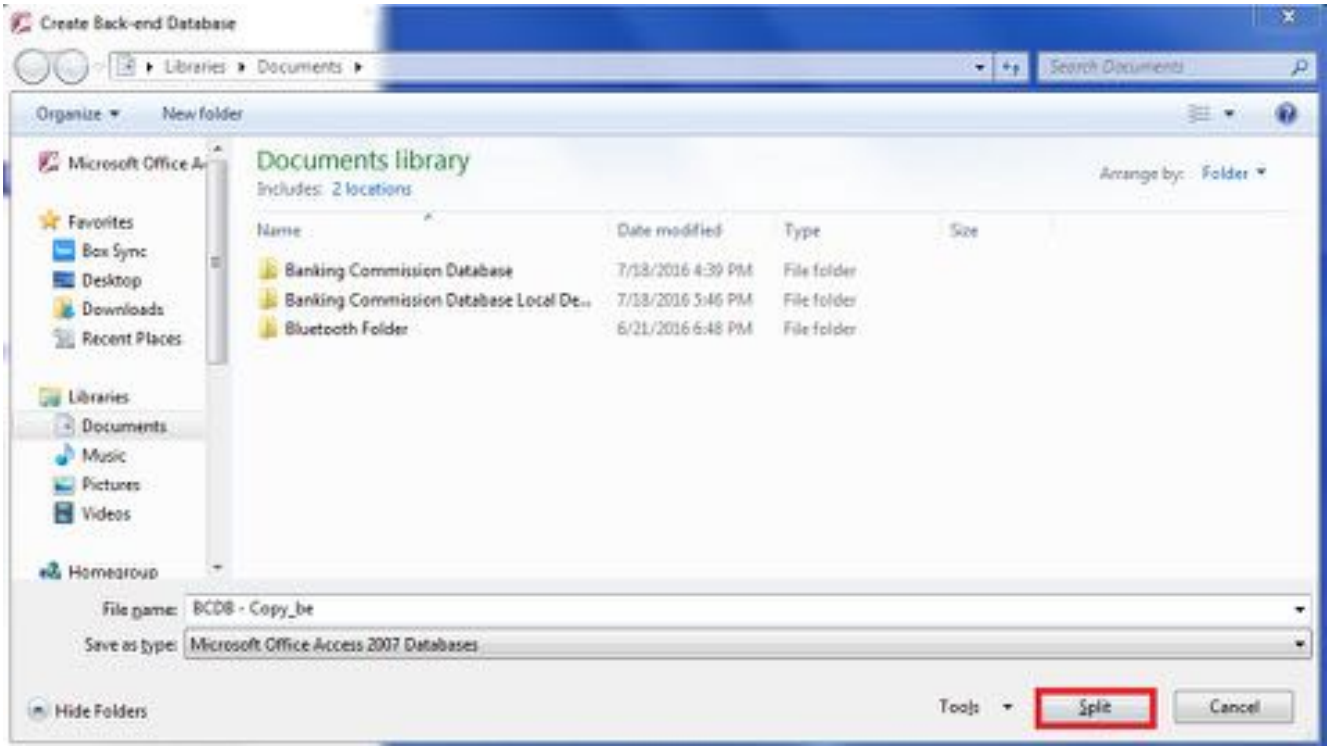
1. On your computer, make a copy of the database file
    - This ensures that if something goes wrong during the process, you have a working version of the database.
2. Open the copy of the database file.
3. Under the **Database Tools** tab, in the **Move Data** group, click on **Access Database**. This opens the database splitter wizard

.

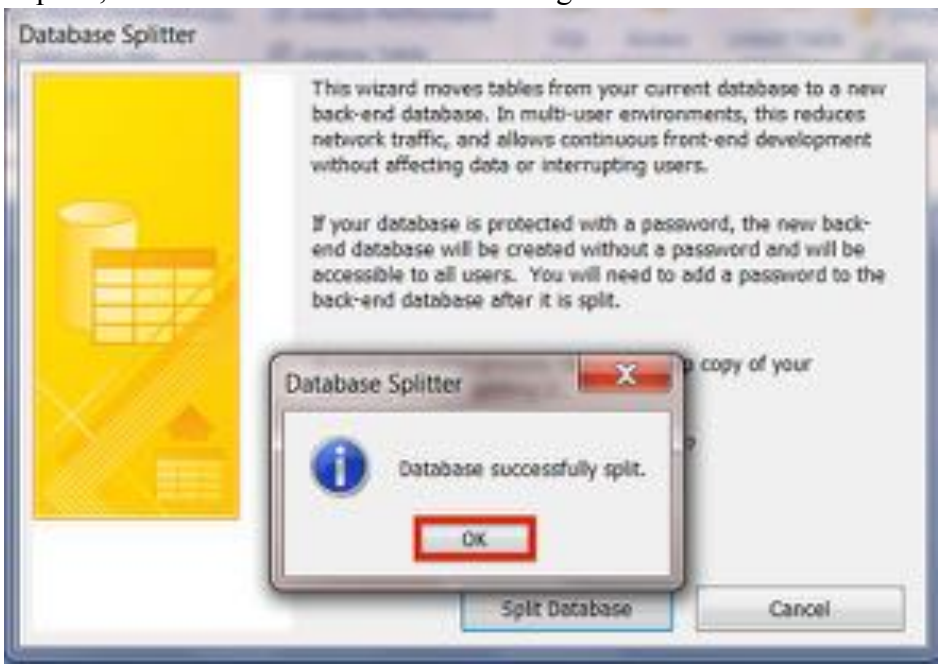
4. Click **Split Database.**



5. In the Create Back-end Database window, specify a file name, database type, and location for the back-end database file.
    - We recommend using the default name and database type that Access recommends.
    - Choose the location for the back-end database file.



6. Once complete, there will be a confirmation message.



7. The database is now split. The front-end database is the file that you initially started with (the copy of the original database). The back-end database is the file that was created in step 5.
8. You can now distribute the front-end database file to each of the users using a usb drive, network shared folders or as an email attachment.

Appendix G.

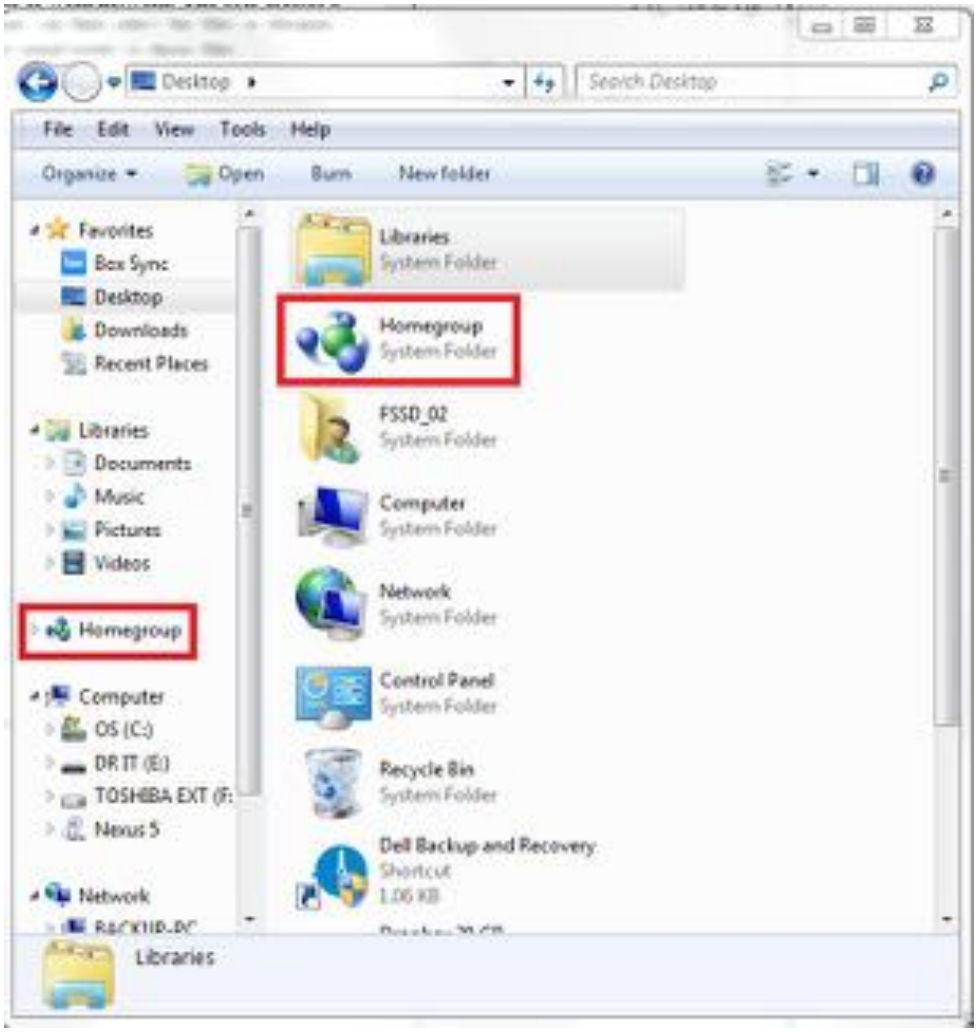
Windows Homegroup and Sharing Files:

In order to share the database, each user should have a copy of the front-end database. However, they need to access the same back-end database file in order to keep the tables consistent. We will use Windows Homegroup in order to share access to the back-end database file.

> A Homegroup makes it easy to share files across a local network. One user creates a Homegroup in its computer and then other users join that Homegroup. Each user can then select the files or folders that they want to share with the other users within the Homegroup, as well as the access level (read or write) to those files.

Joining the Homegroup and Sharing Files:

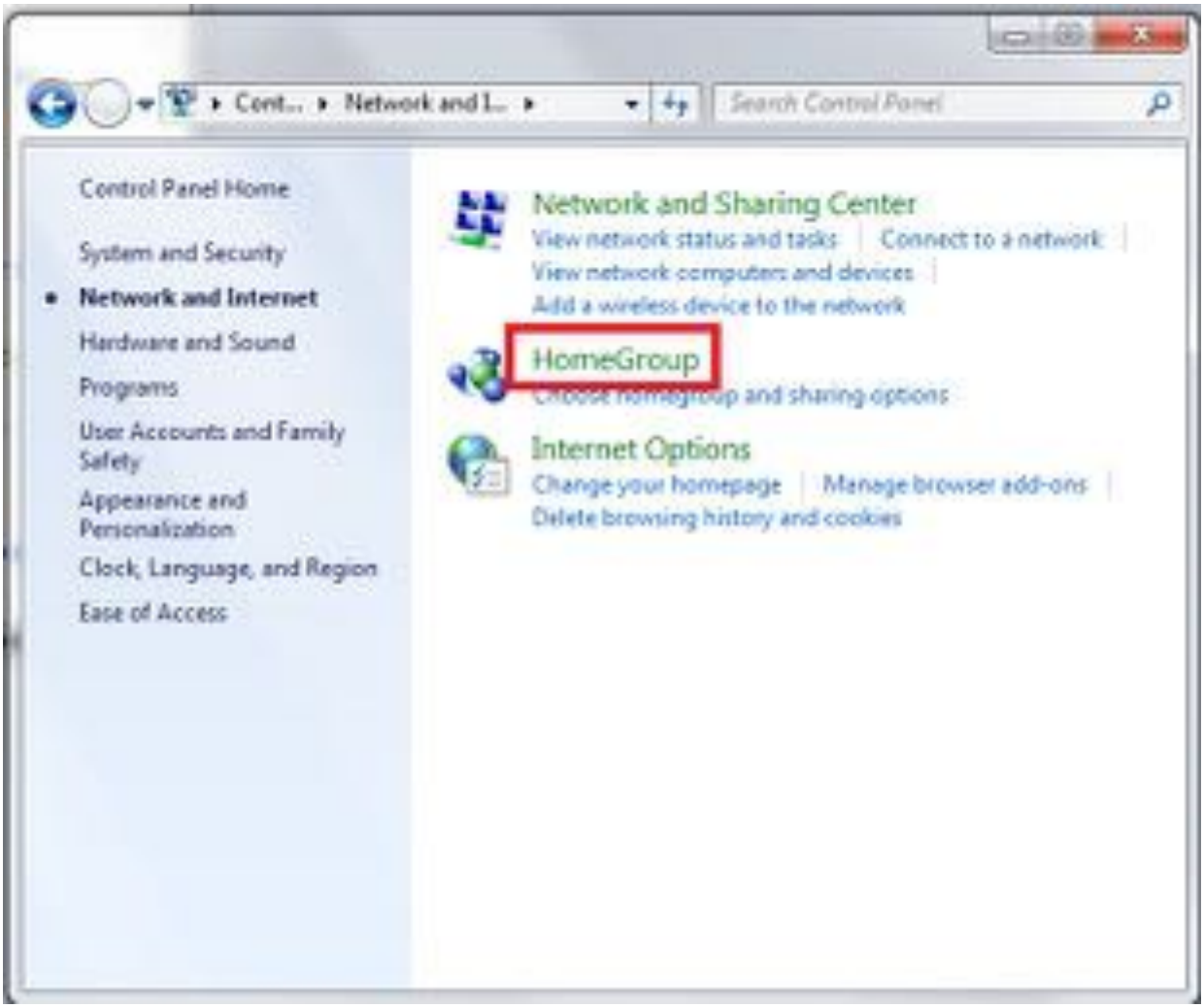
1. Click on the **Homegroup** tab in the Windows Explorer



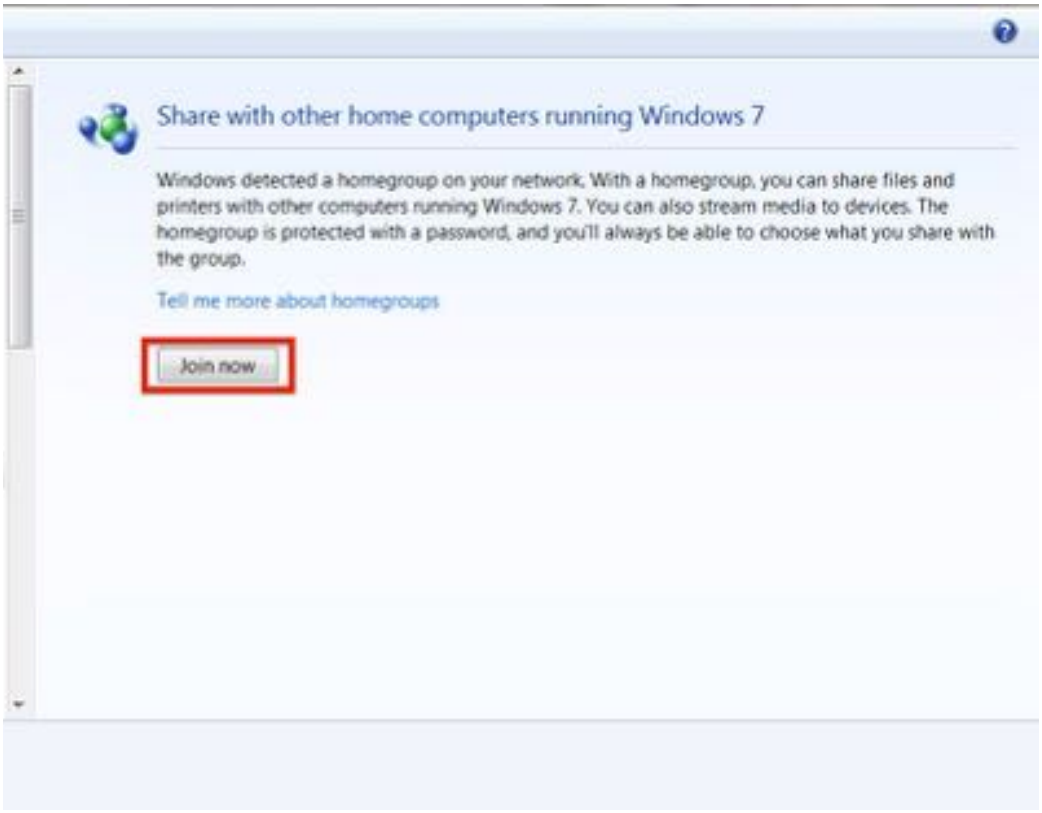
Note: If it does not appear on the Windows Explorer, click on Control Panel in the Start Menu

Then click on **Network and Internet**

Then on **HomeGroup**



2. There should be a message that your computer has detected a Homegroup on the network. Click **Join now**



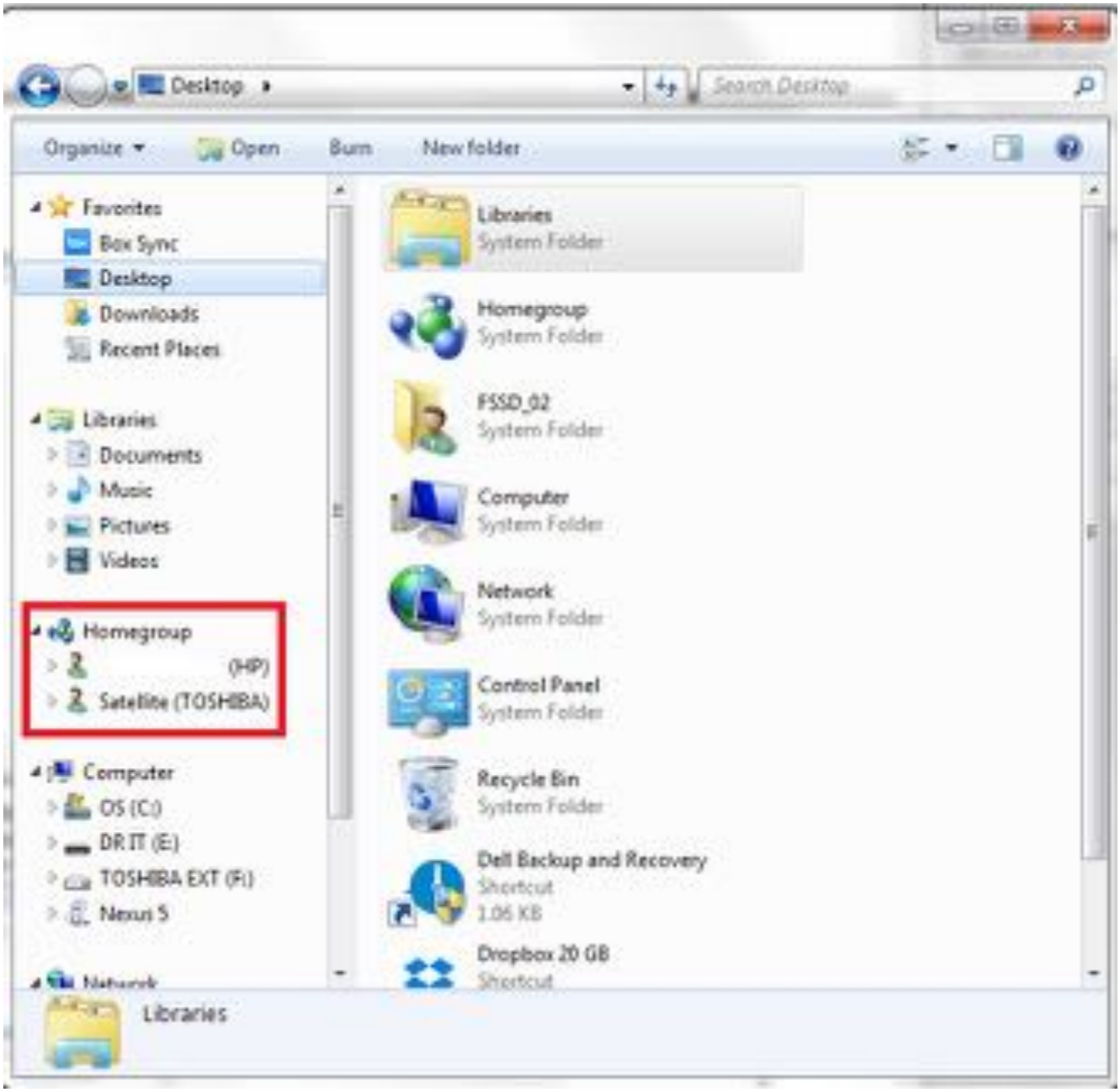
3. Select what you want to share with the Homegroup. We recommend sharing only **Documents.** Click **Next**.

- Only the computer that is sharing the back-end database needs to share **Documents**. The other computers do not have to share anything.
- This means that any files that are in the folder **Documents** will be shared to the other computers within the Homegroup

4. Enter the Homegroup password.
   Click **Next**

5. A confirmation message will appear
   Click **Finish**

6. Under the **Homegroup** tab in **Windows Explorer**, you can now see all computers that are currently connected to the **Homegroup**

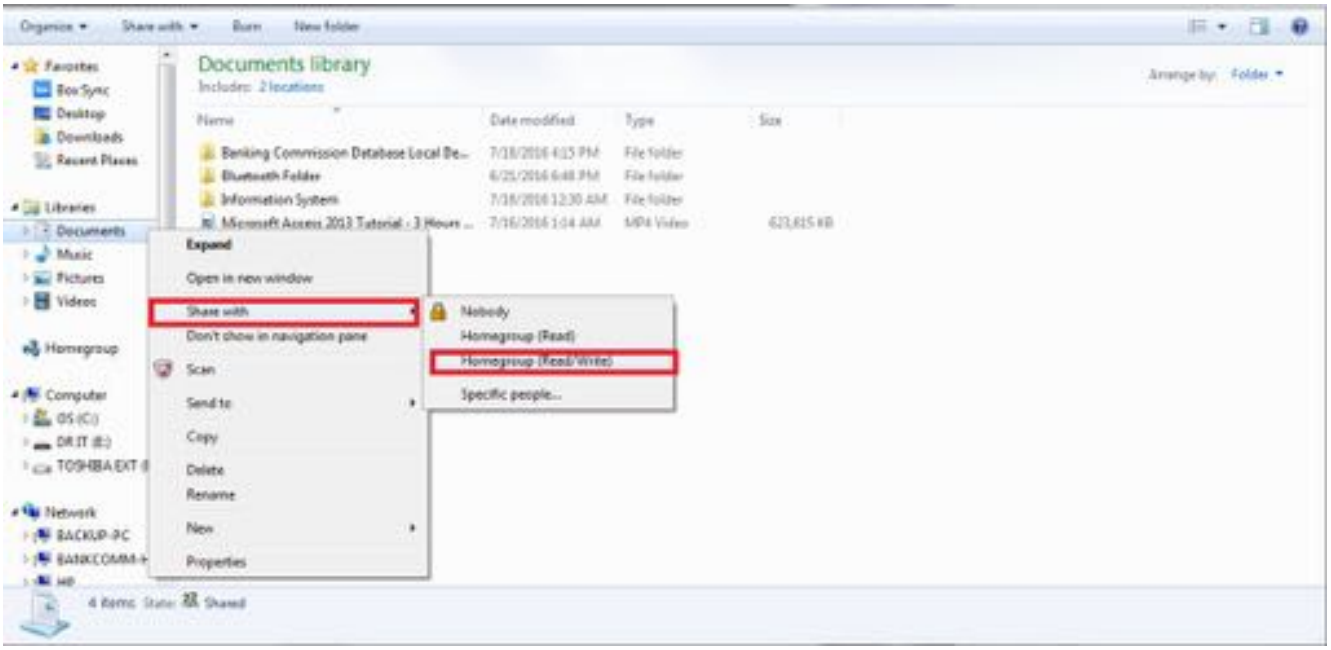


7. Once you click on one, you can view the files currently being shared by that computer with the Homegroup

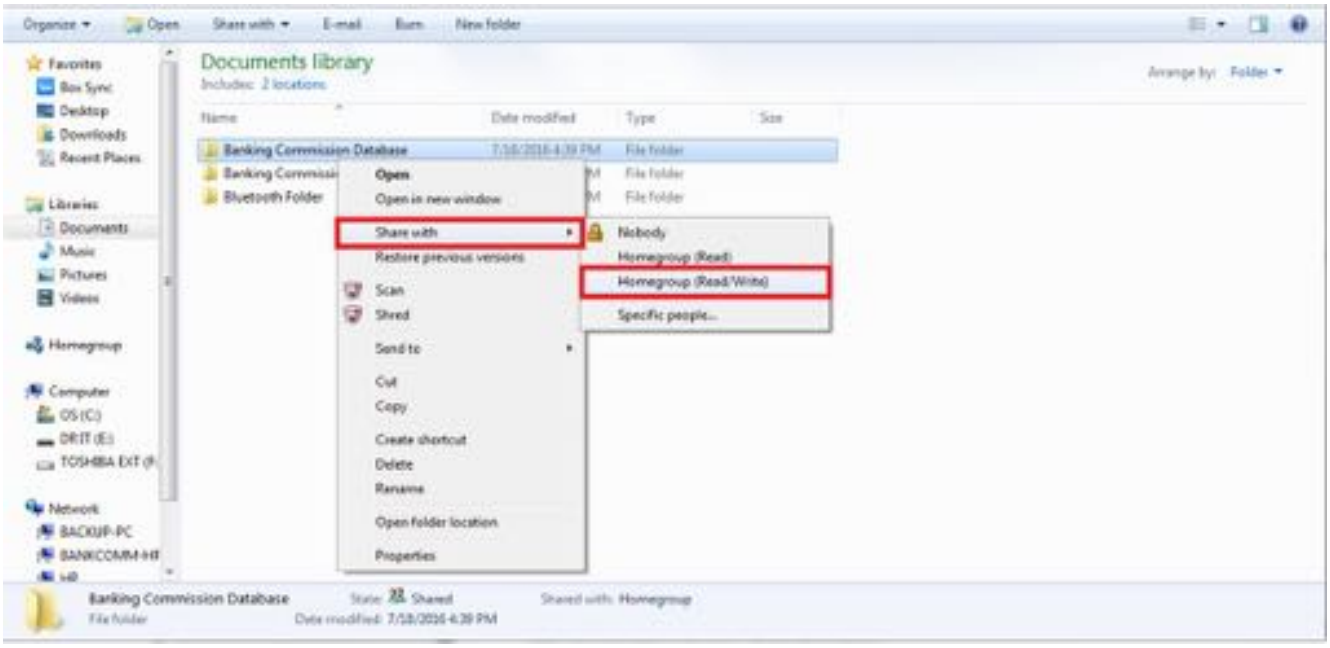
Sharing the back-end database file:

1. Right-click on **Documents** folder and click on **Share with** -> **Homegroup (Read/Write)**

- This will ensure that all the files in this folder can be viewed and modified by other members of the homegroup.
- If there are certain files that you do not want to share, click on **Share with** -> **Nobody.**



2. Create a folder called **Banking Commission Database** in the **Documents** folder, if it does not exist already
    - This will be the location for files to share with the homegroup
3. Right-click on **Banking Commission Database** and click on **Share with** -> **Homegroup (Read/Write)**
    - This will ensure that all the files in this folder can be viewed and modified by other members of the Homegroup



4. Move the back-end database file into the **Banking Commission Database** folder.
5. Right-click on the back-end database file and click on **Share with** -> **Homegroup (Read/Write)**

6. The files can now be viewed and modified by others members of the Homegroup

Where to find the back-end database files for other users:

1. Under the Homegroup tab in the windows Explorer, you can see all of the computers that are currently connected to the Homegroup

2. Navigate to the back-end database file **BCDC - Copy_be**, which is located in the **Banking Commission Database folder**
3. Now you can link the front-end to this back-end database file.
    - In order to access the back-end database file, the computer that is sharing it **MUST** be **ON** and connected to the **Homegroup**
    - In order to modify the contest of the database (update tables, input new data, etc), the back-end database file **MUST** be shared with **read/write** access to the **Homegroup**

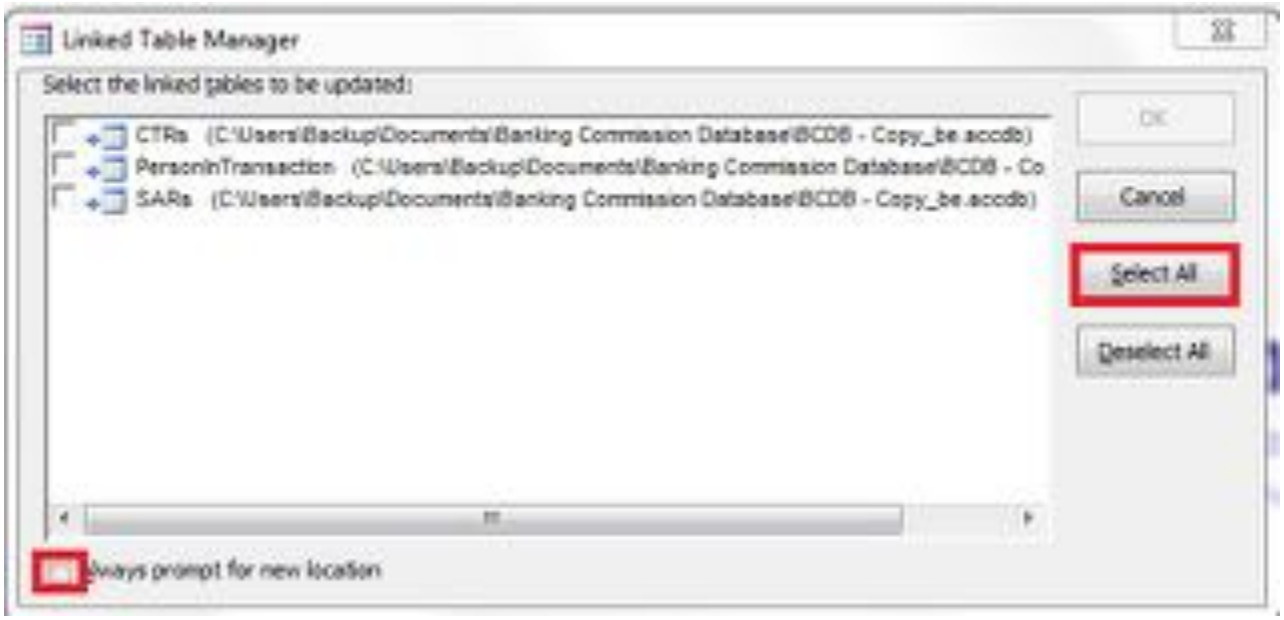
Appendix H.

Linking an Access database:

Now that the database is split each user has a copy of the front-end database file. We need to link that front-end database file to the back-end database in order to access/edit the data tables.

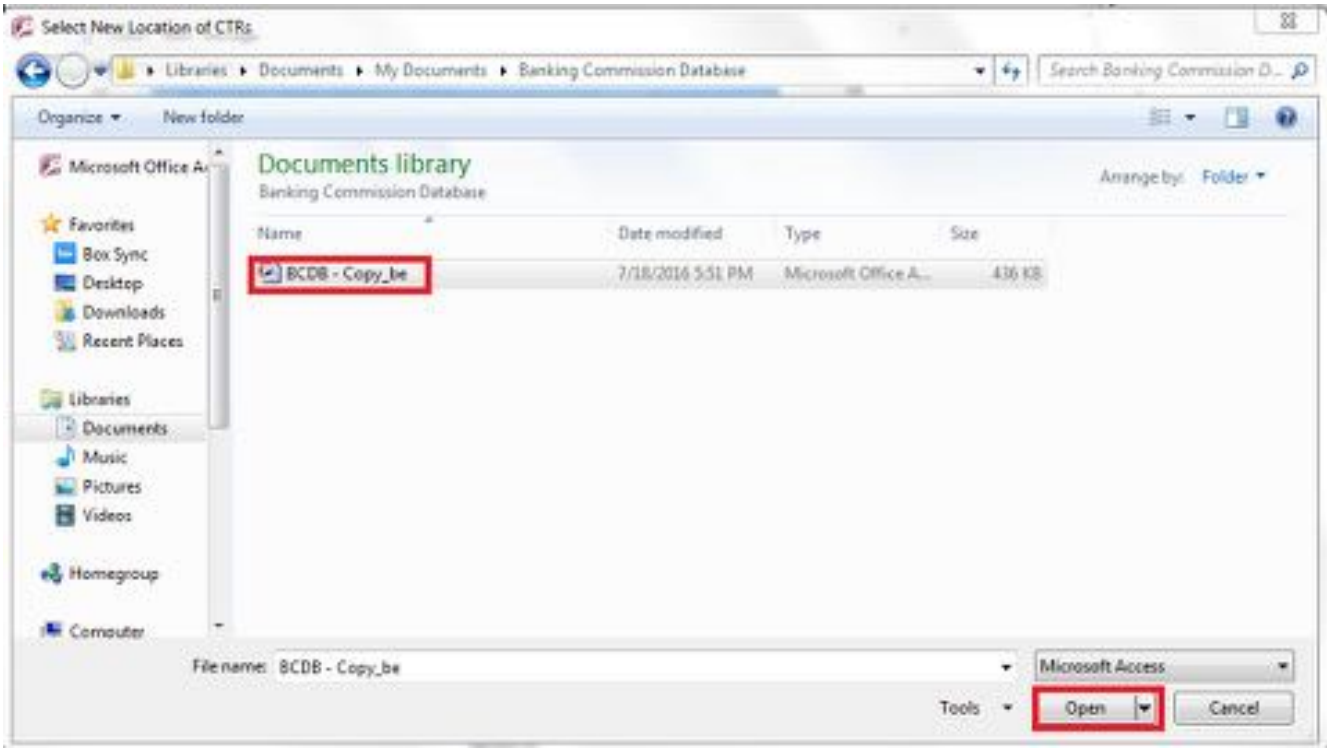
1. Open the front-end database file.
2. Under the Database Tools tab, in the Database Tools group, click Linked Table Manager.

3. Click **Select All** in order to relink all of the data tables. In order to choose the location of the back-end database, click the checkbox for **Always prompt for new location**.
    - If you want to relink only a single table, then click only on that table's selection box



4. Click **OK**.

5. Navigate to the location of the back-end database file and select it. Click **Open.**



6. The front-end database is now linked to the back-end database.
    - This allows the user to be able to use any forms, queries, or reports in the front-end database that are associated with the back-end database data tables.

Appendix I.

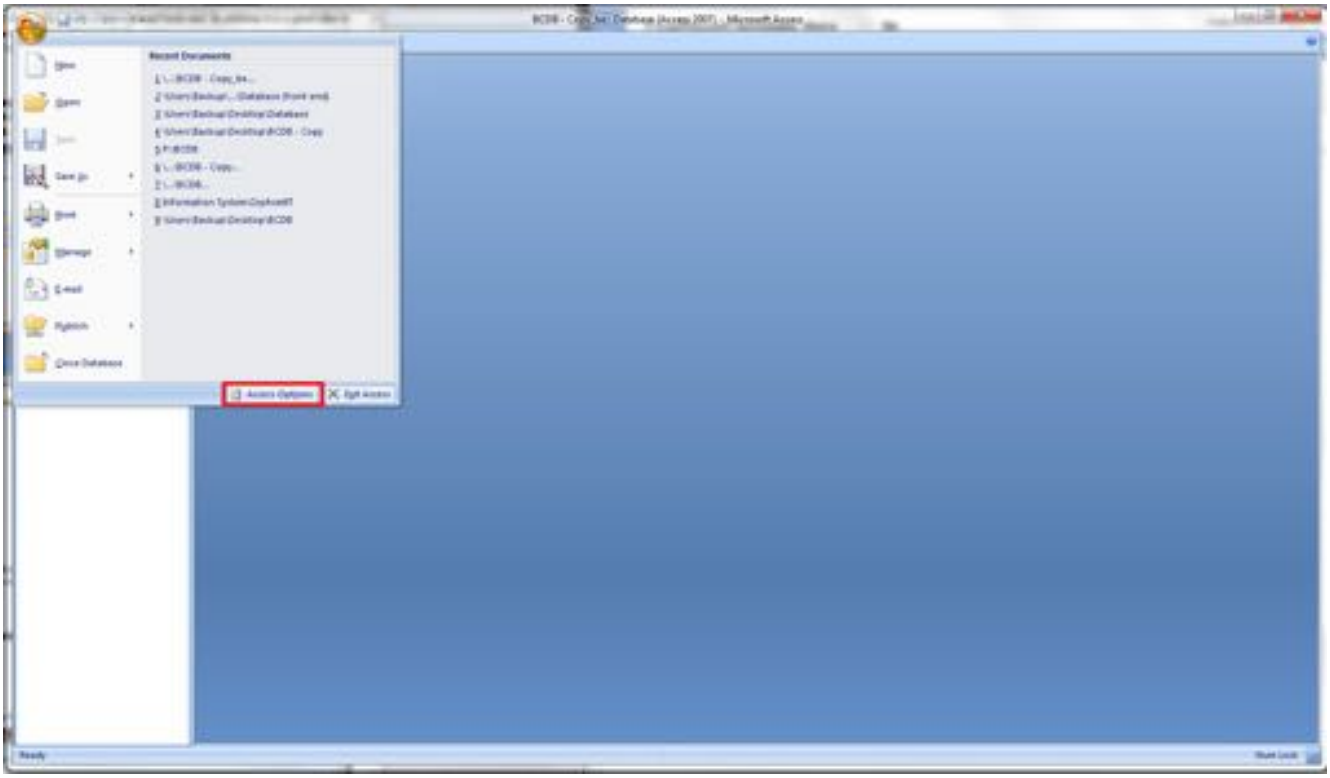
2GB Access Database Size Limits:

Microsoft Access has a size limit of 2GB for databases files. In order to avoid running into issues with the size limit, a good practice is to split the database into a front-end and back-end, as it was detailed previously. Additionally, it is a best practice to compact and repair the Microsoft Access database after use. As the database grows in size (more records being imported/typed), Access keeps temporary files and deleted data behind the scenes. In order to free up this space, we need to compact and repair the database.

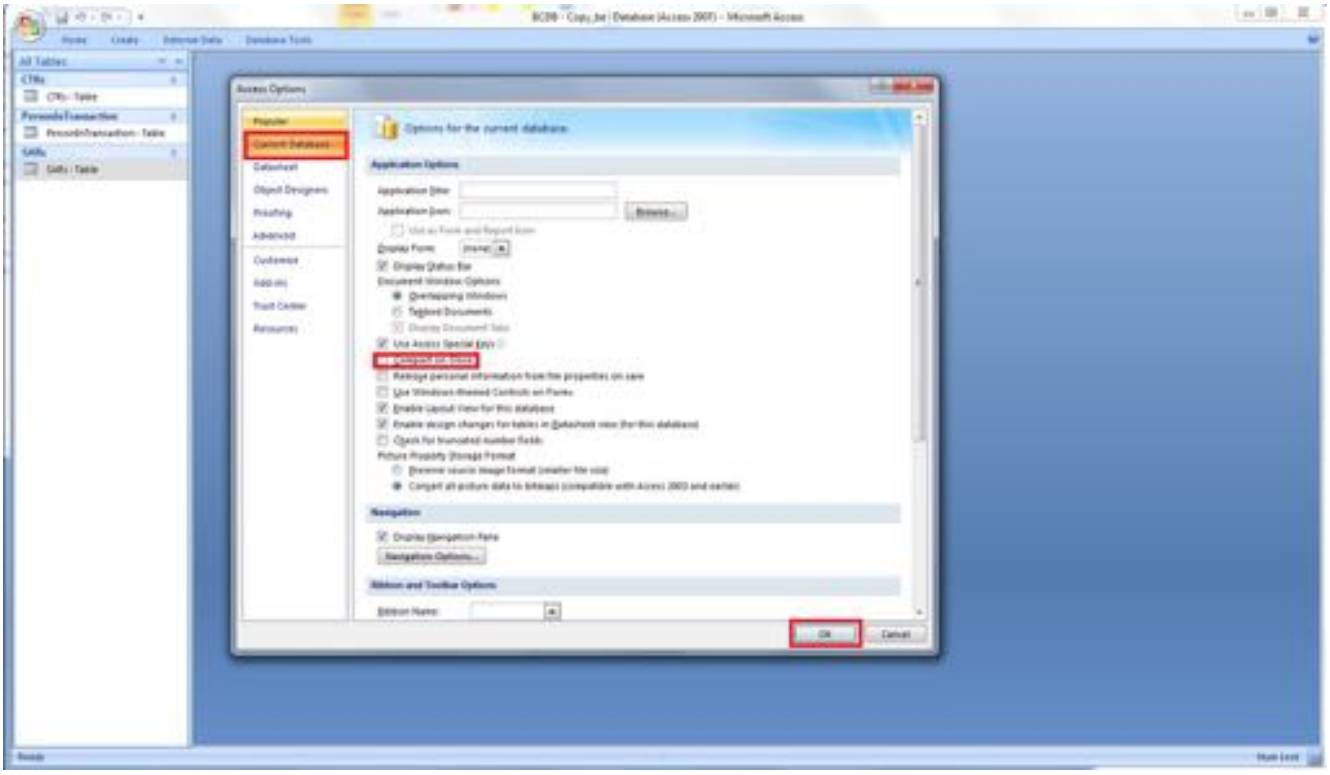
Automatically Compacting and Repairing the database:

The following steps should be repeated for the back-end and front-end database file if the database has been already splitted

1. Open the Microsoft Access database
2. On the **File** tab, click **Access Options**



3. In the **Access options** dialog box, click **Current Database**. Then check the option **Compact on Close**
   Click **OK**



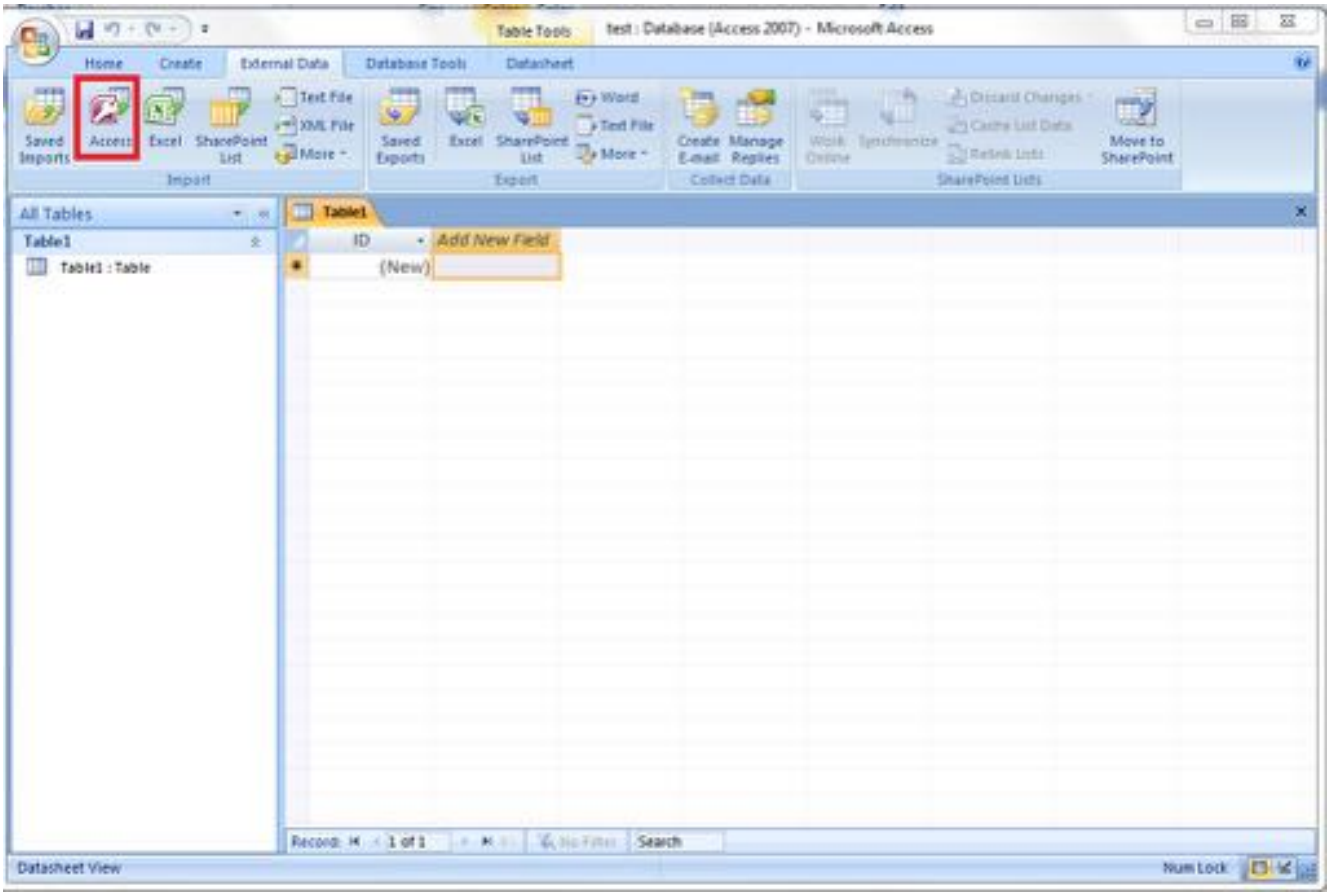
4. From now on, each time you close the database, Microsoft Access will automatically compact and repair the database.

Note:

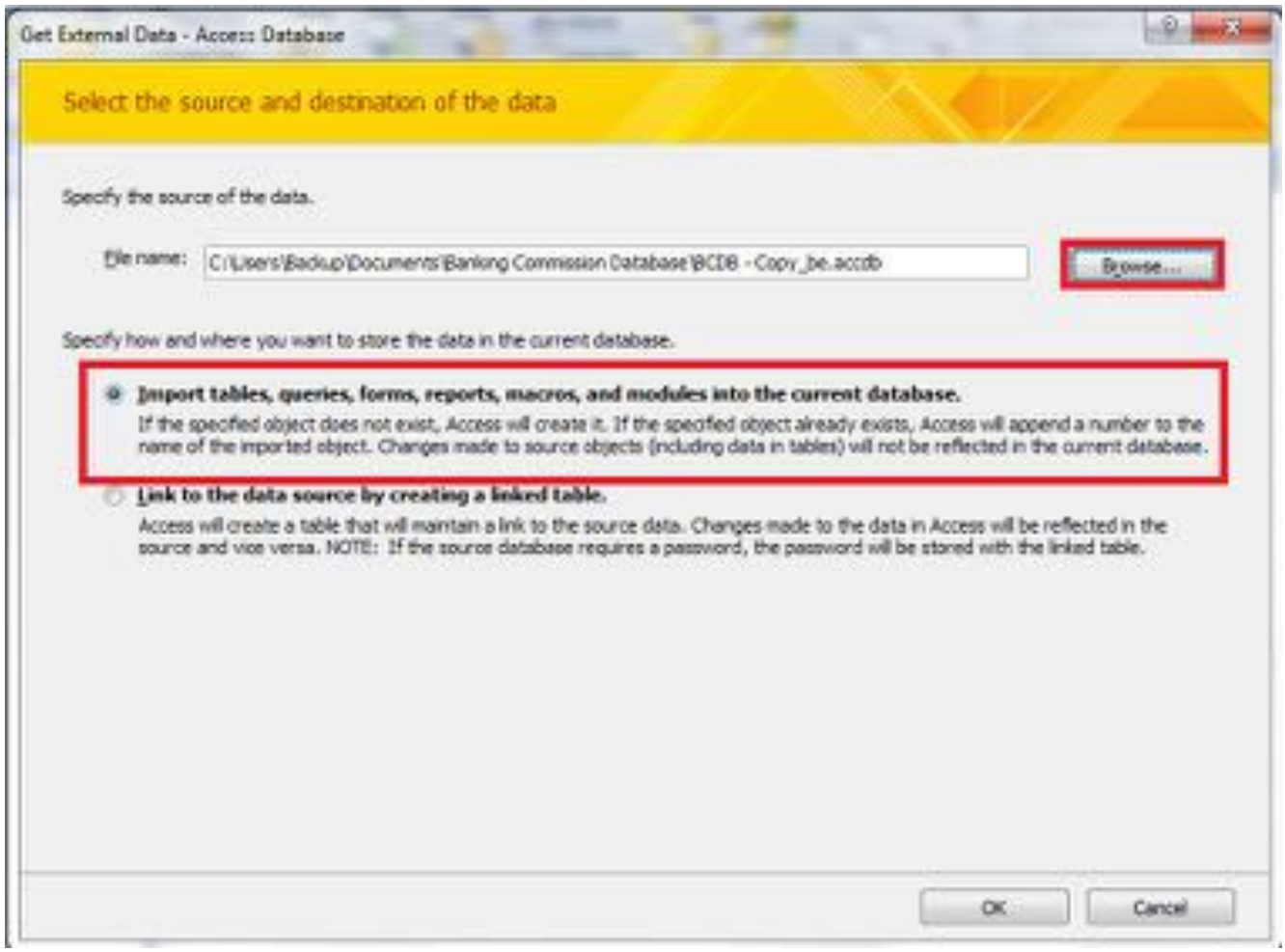
If the database is approaching the 2GB database size limit, the next best practice is to split each data table into its own file and relink the database. With this setting, now each table can be up to 2GB whereas before, the sum of all tables could only add up to 2GB. However, this scenario is unlikely since each CTR and SAR only represent one record in the tables. Unless the number of reports filed grows dramatically there will be no immediate need of performing this configuration.

Moving Each Table to Own File and Relinking:

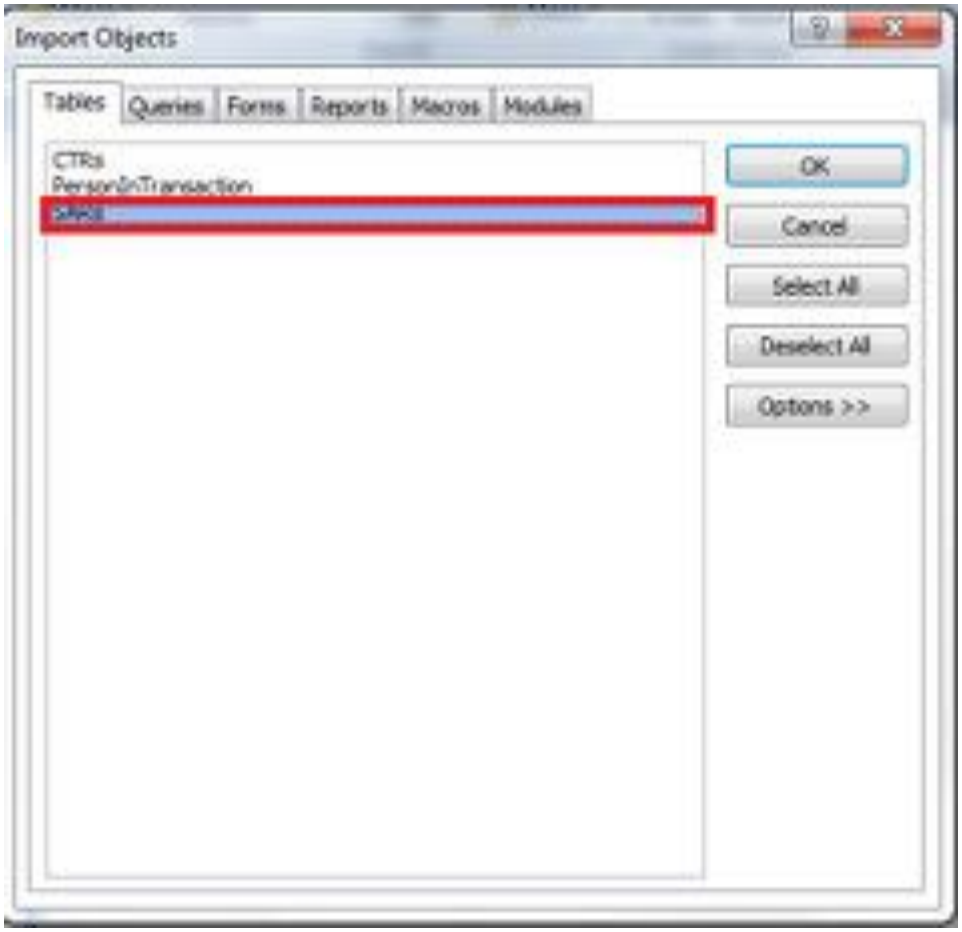
1. Create a new Blank Database in Microsoft Access
2. Under the **External Data** tab, in the **Import** group, click **Access**



3. Select the back-end database file to import the table from using **Browse …**
4. Select **Import tables, queries, forms, reports, macros, and modules into the current database**.
   Click **OK**



5. Select the table to import and click **OK**



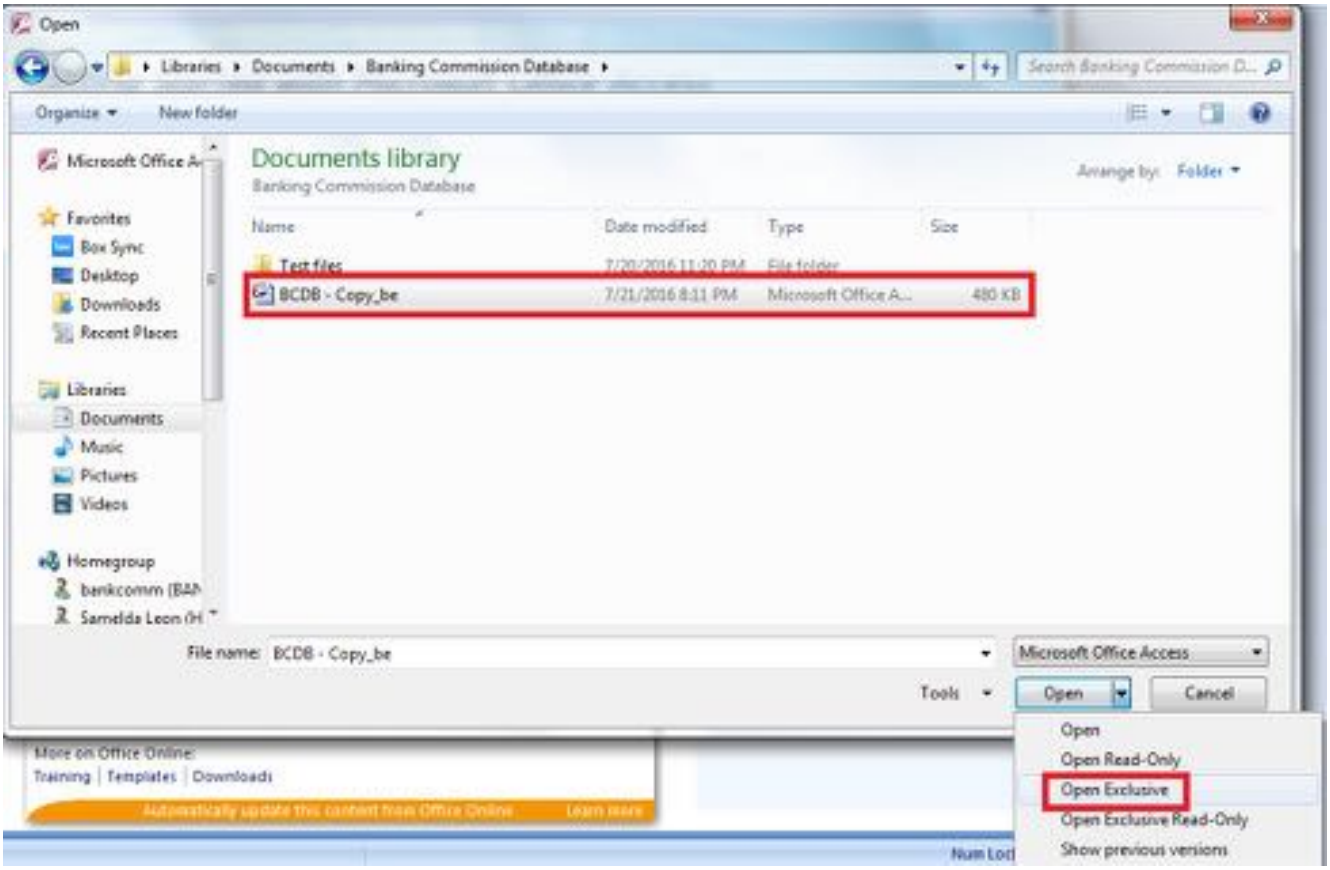
6. When the confirmation message appears, click **Close**
7. The database has now the imported table. Repeat steps 1-7 for each table in the back-end database file
8. Relink each table (that now are independant database files) with the front-end database.

Appendix J.

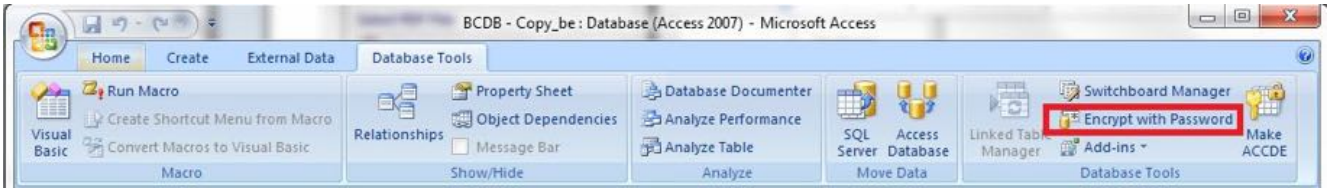
Encrypting/Decrypting an Access Database

In order to ensure the security of the Microsoft Access database, it is necessary to encrypt it. Essentially, this means protecting the database with a password; meaning that if someone does not have the password, they cannot use the database or see its contents.

1. Open the database file in **Exclusive** mode

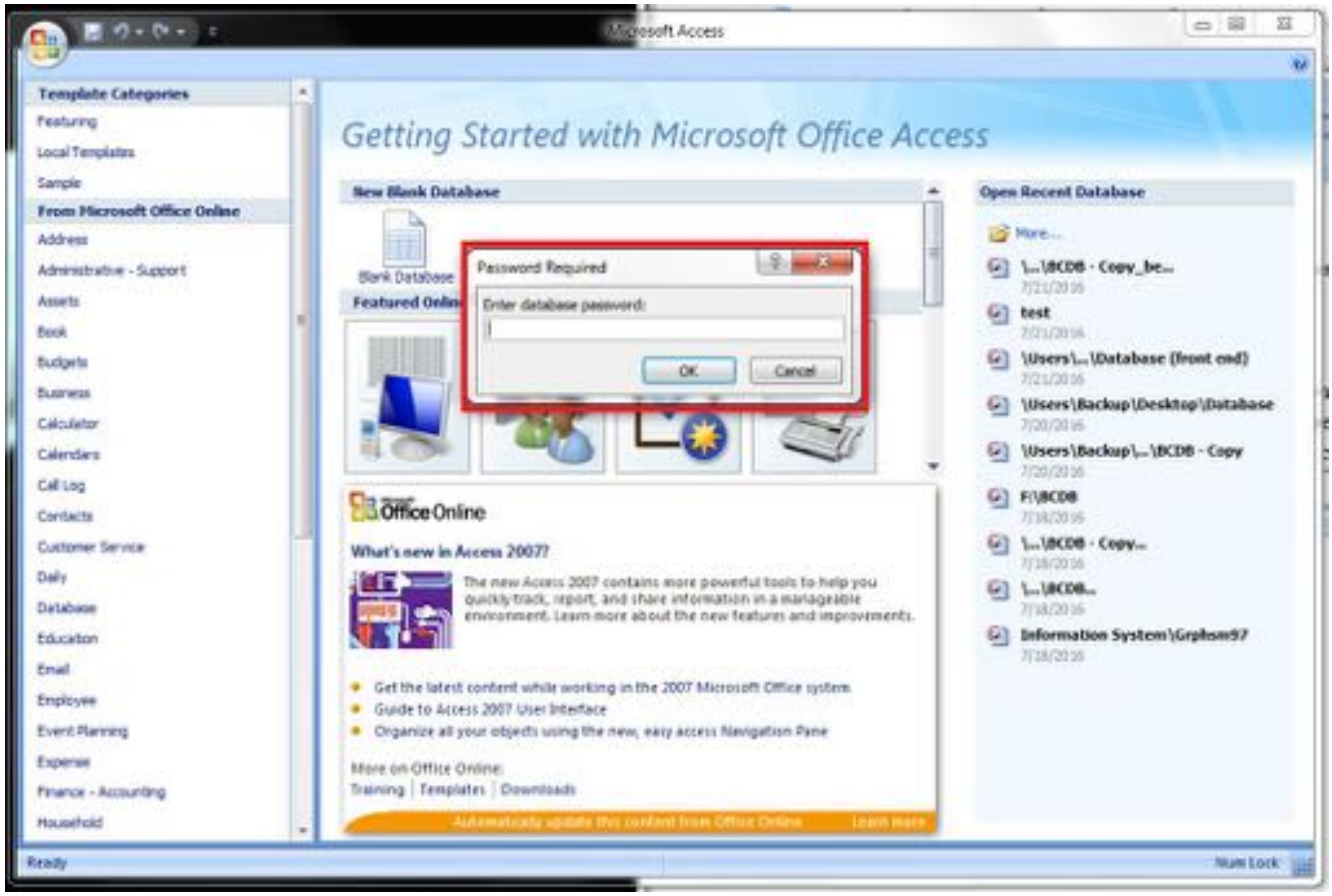


2. Under **Database Tools** tab, in the **Database Tools** group, click **Encrypt with Password**

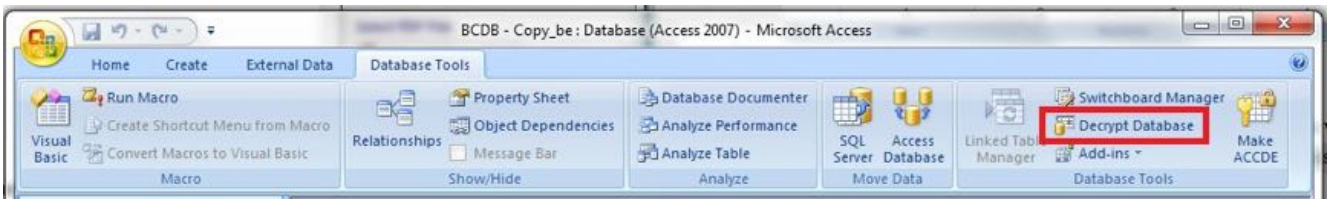


3. Enter the new password
    - Use a strong password by combining uppercase and lowercase letters, numbers, symbols, and at least 8 characters in length
    - Strong password example: a90!_%bD
    - Weak password: bankcomm2016
    - Write down the password and store it somewhere secure, until it is memorized. **DO NOT** store the password on the same computer that has the database
    - If you **FORGET/LOSE** the password, the database **CAN NO LONGER** be accessed. Then click **OK**

4. From now on, every time you open the database you will be required to enter in the password



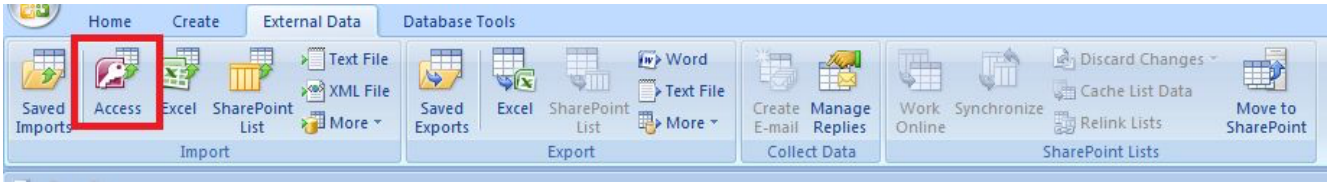
5. If you need to decrypt the database, such as to change the password, under the **Database Tools** tab, in the **Database Tools** group, click **Decrypt Database**
   Note: In order to decrypt the database, the database file should be open in **Exclusive** mode (step 1)



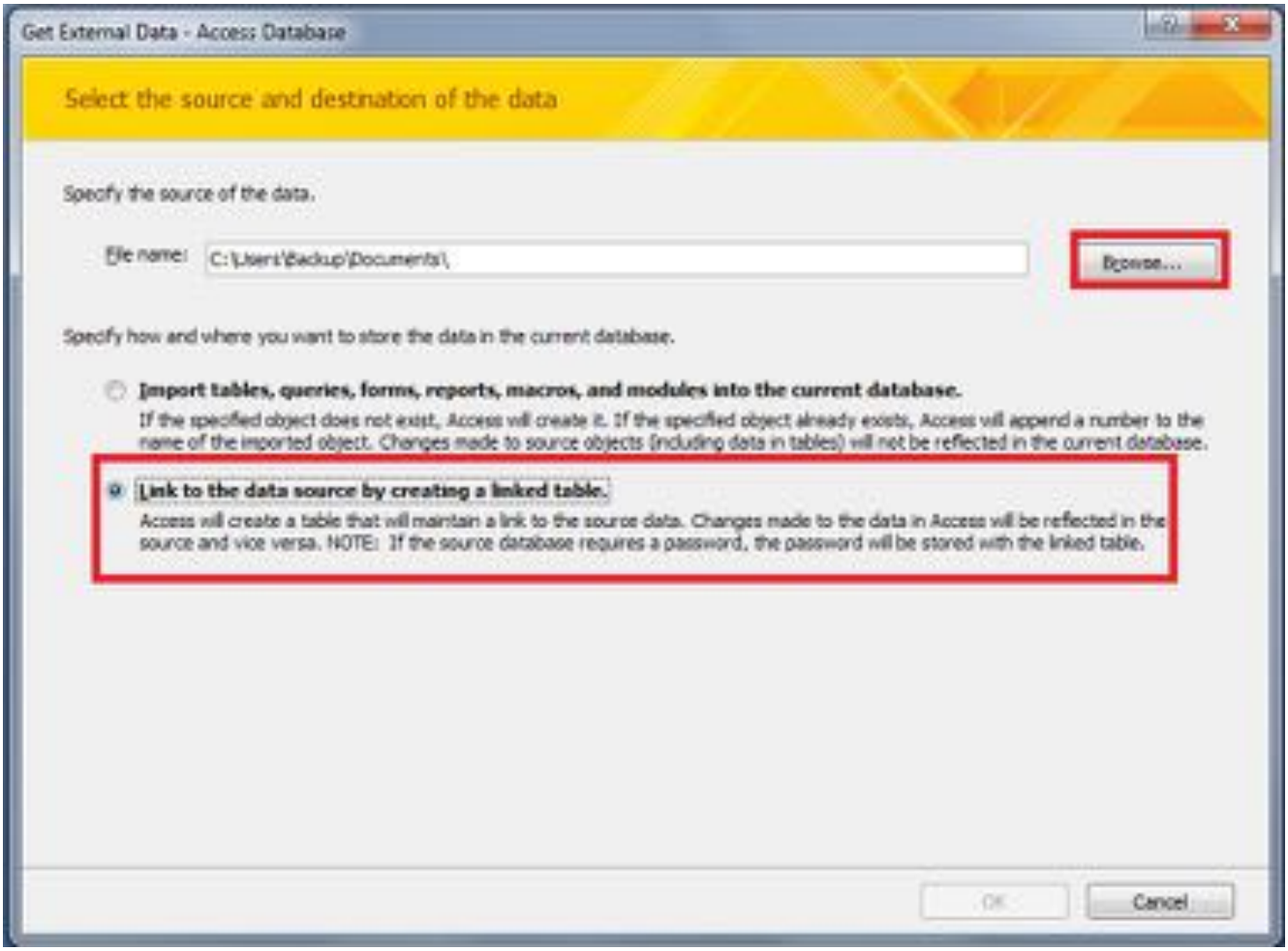
6. Enter in the current password and click **OK**
   - The database is no longer encrypted and can be opened without the previous password

Encrypting a split Access Database

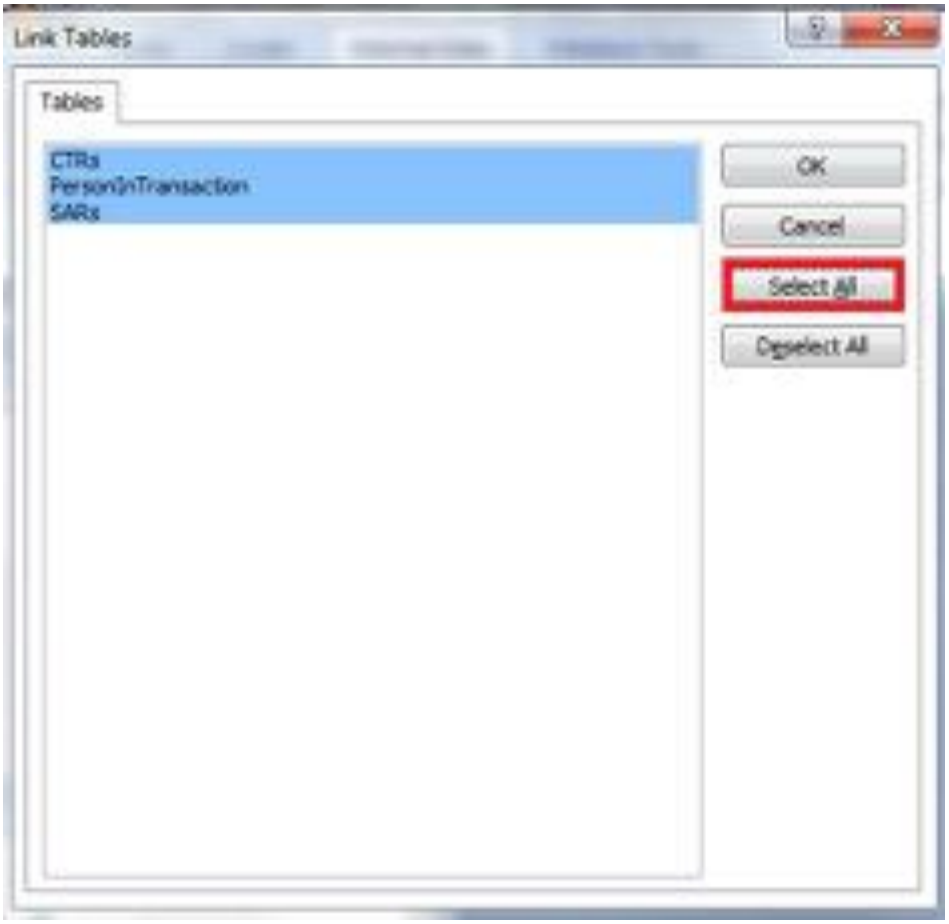
1. Encrypt the back-end database
2. Open the front-end database and delete the linked tables (the ones with the arrowhead in front of the icon)
3. Under the **External Data** tab, in the **Import** group, click **Access**



4. Select the back-end database file to import the table from using **Browse …**
5. Select **Link to the data source by creating a linked table**.
   Click **OK** and enter the password of the back-end database file



6. Click on **Select All** and then **OK**



7. Open the front-end database in **Exclusive** mode and proceed to encrypt it. A different password can be used for the front-end

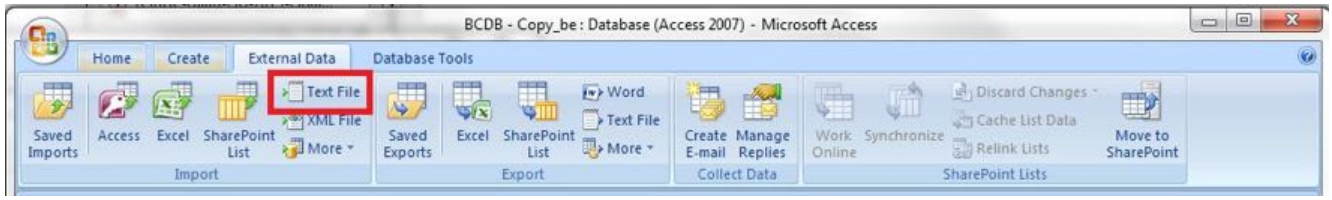
Appendix K.

Import CSV Files into Access Database

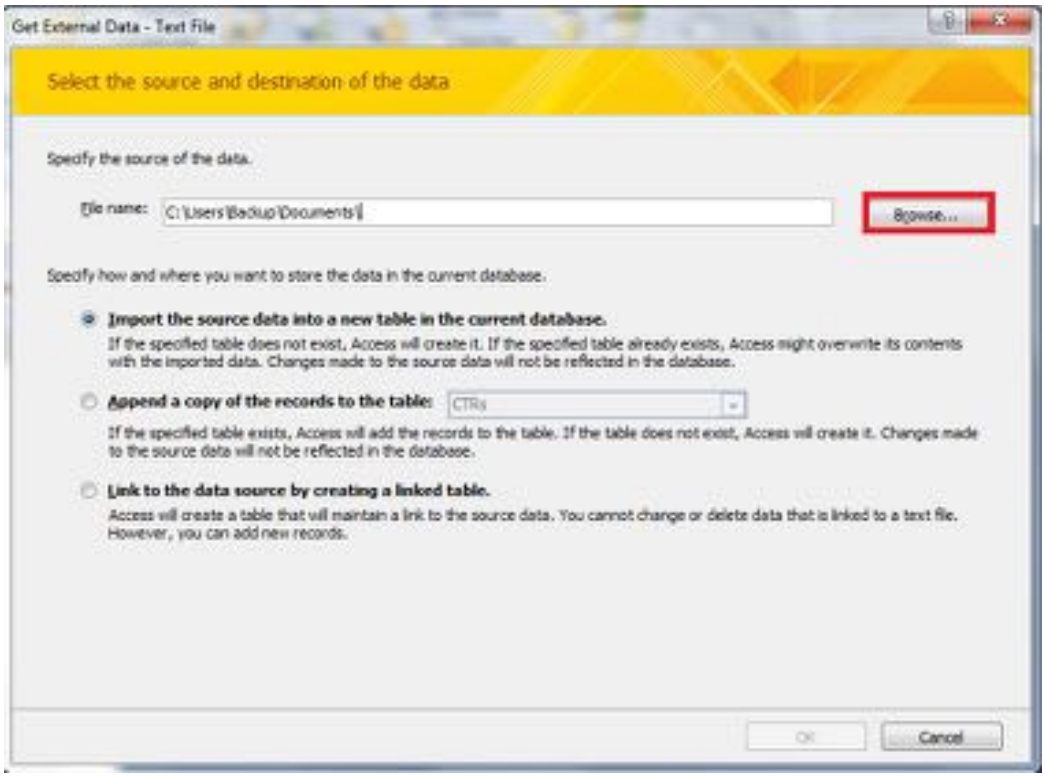
Once the CSV files are downloaded onto the user's computer, they **MUST** be imported into the database.

Note: They MUST be imported directly into the BACK-END database file, NOT the front-end database copy.

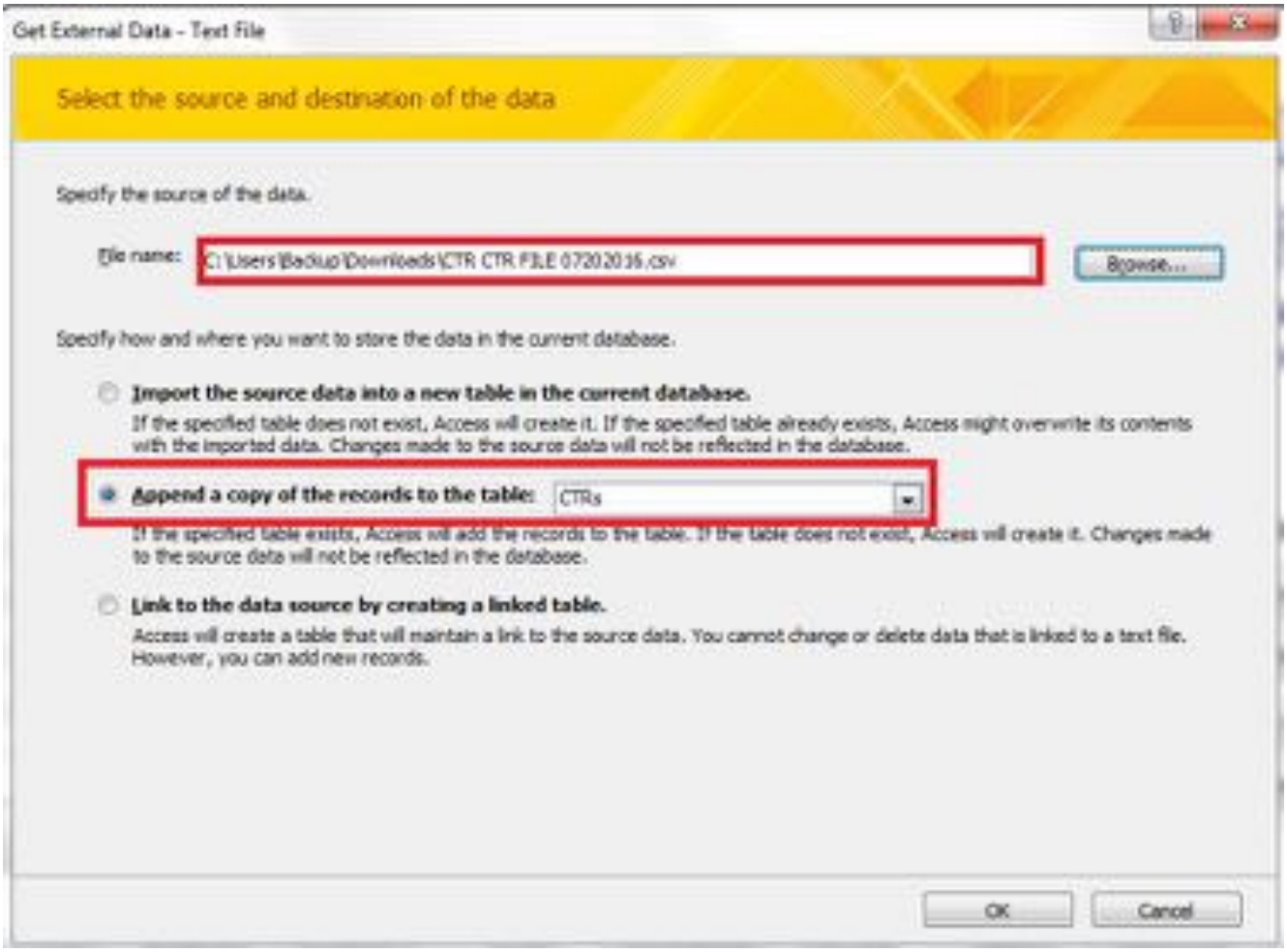
1. Under the **External Data** tab, in the **Import** group, click **Text File**



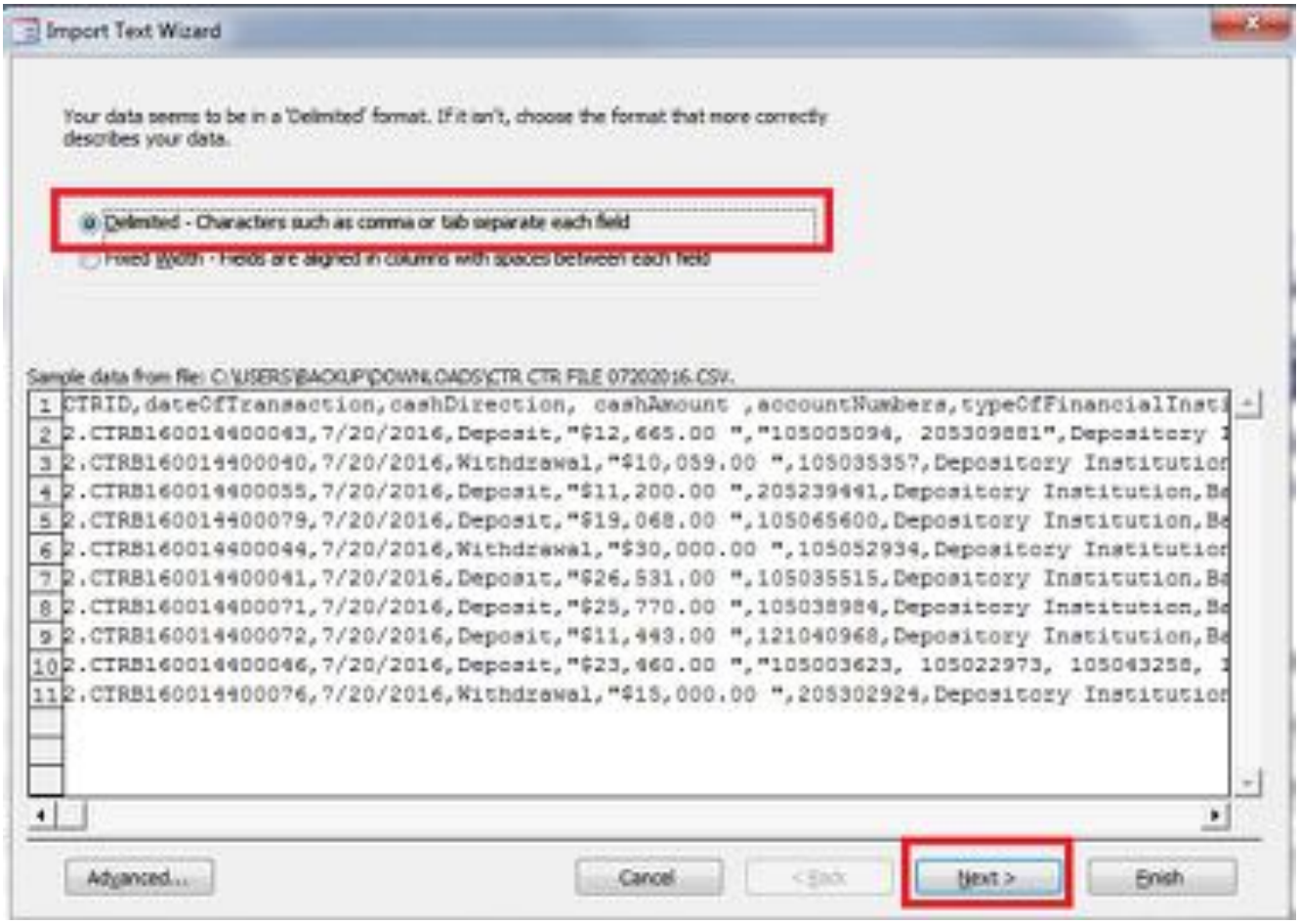
2. Click **Browse…**



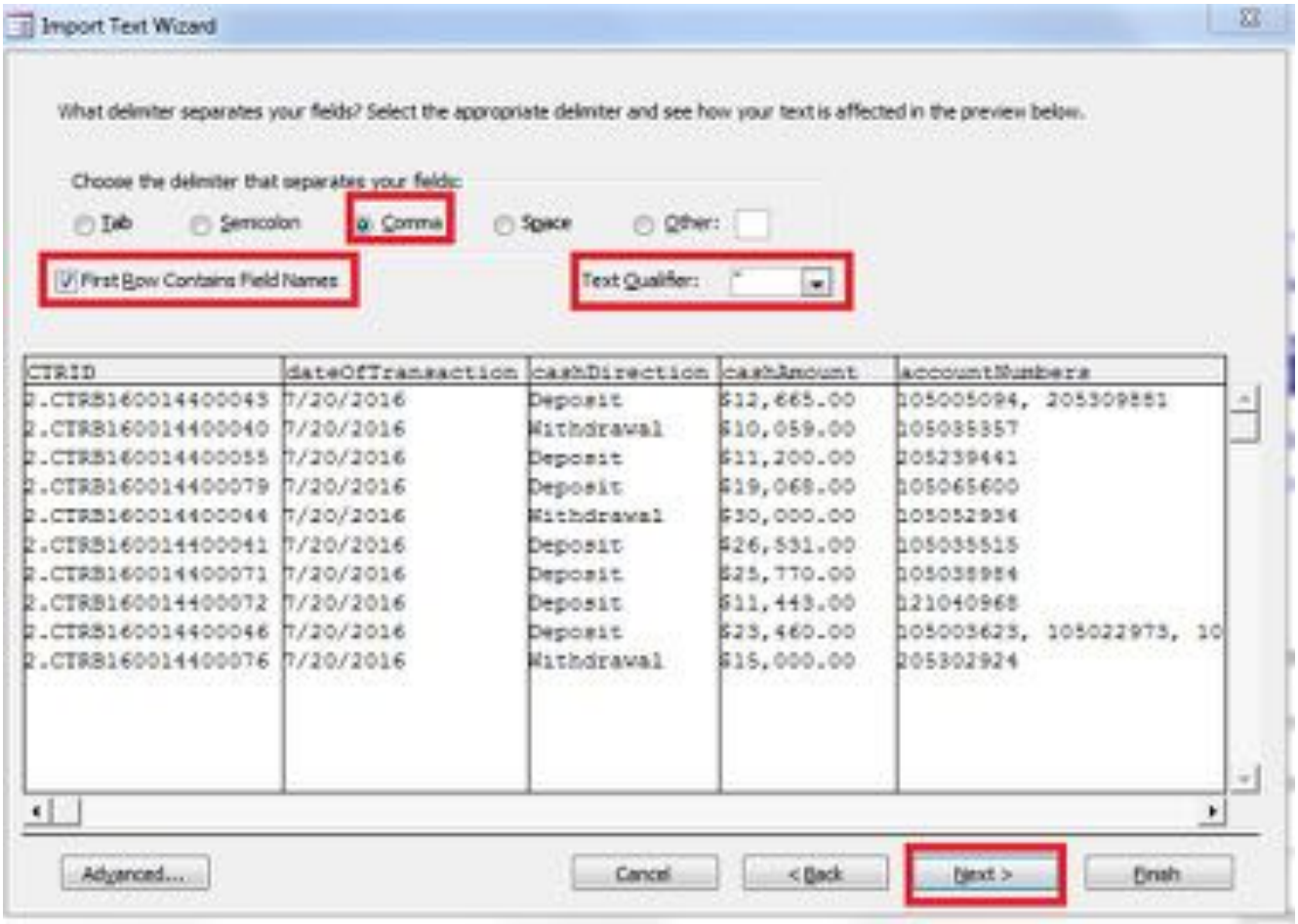
3. Navigate to the location of the CSV file and select it. Click **Open**
4. Choose **Append a copy of the record of the table** and then select the table from the dropdown list that matches the CSV file (i.e. a CSV file with CTR information should be appended with the CTRs table). Click **OK**
   Note: If "Import the source data into a row table in the current database" (default choice) is selected by mistake, ALL previous data of the matching table will be OVERWRITTEN.



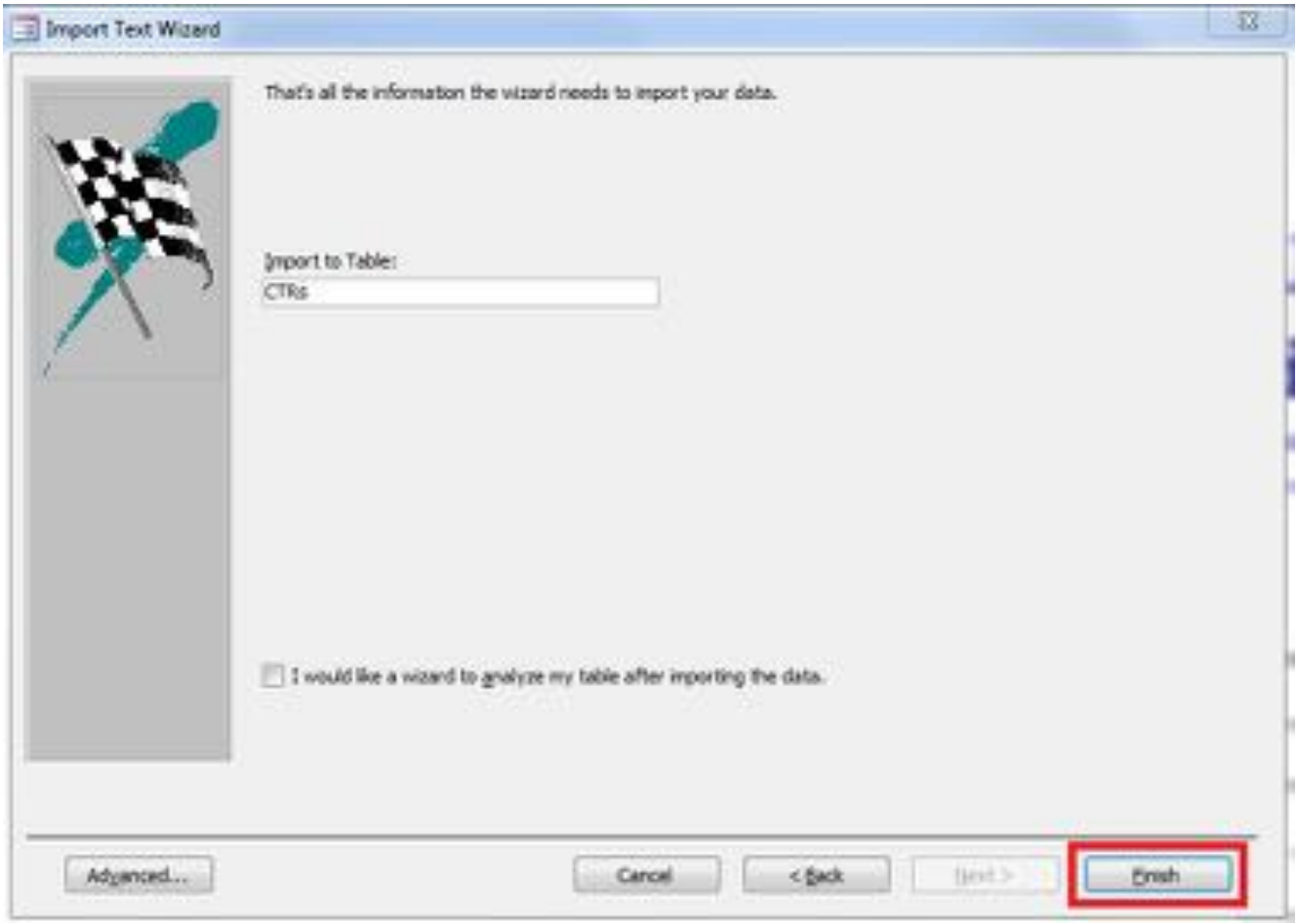
5. Choose **Delimited - Characters such as comma or tab separate each field**. Click **Next**



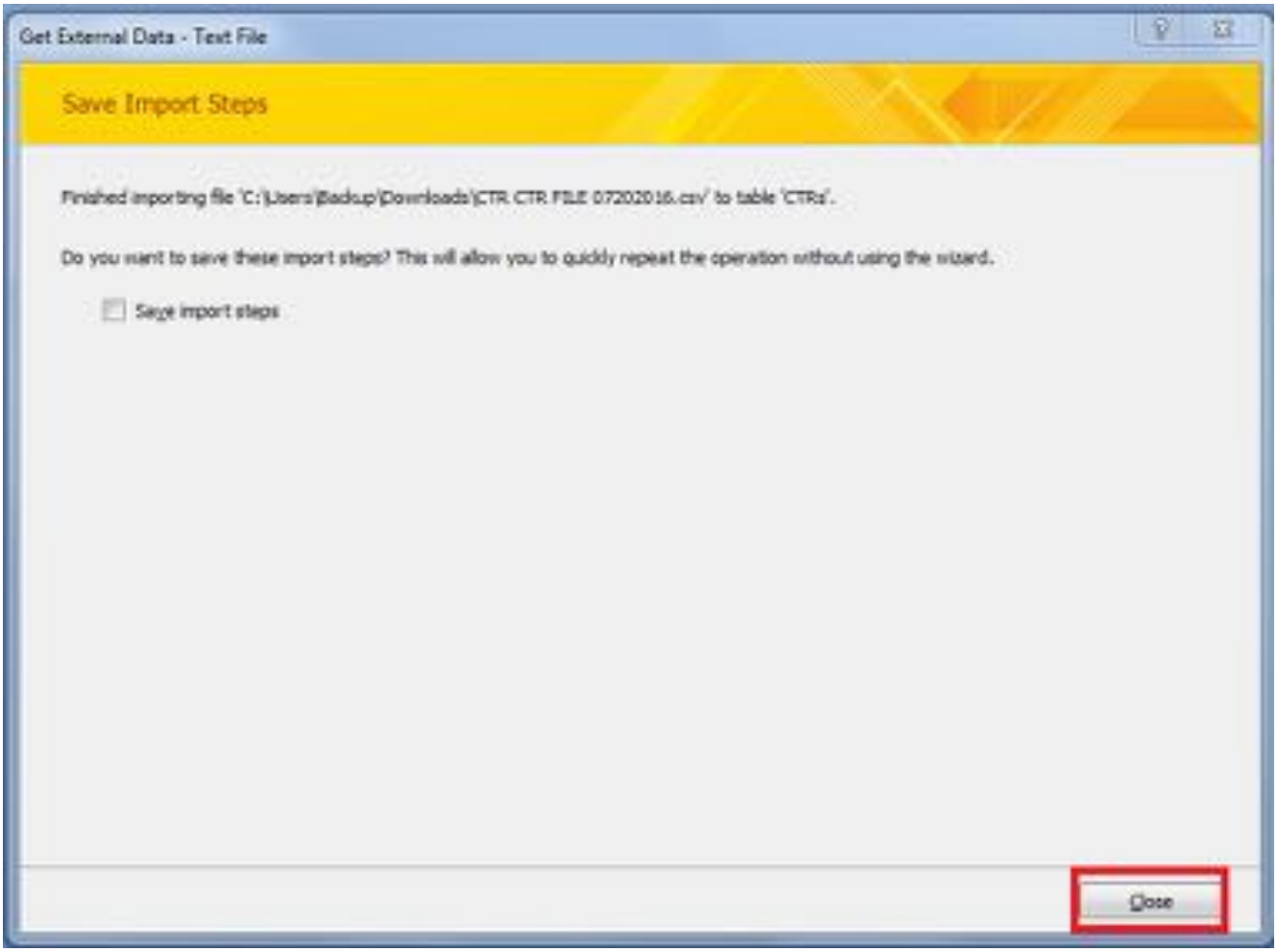
6. Select **Comma** as the delimiter to separate the fields. Also, select **First Row Contains Field Names**. Finally, select double quotes " as the **Text Qualifier.** Click **Next**.



7. Click **Finish**



8. Click **Close**



Appendix L.

Website Cost Decision Diagram

	Website Builder	**Domain**	**Email**	**Total cost for 36 months**
WordPress	$ 99/year	Included	Does not included - Can use Zoho	$ 297
GoDaddy	$ 3.99/month	Included	Included 1 free for the first 12 months	$ 143.64
BlueHost	$ 3.95/month	Included	Included 5 with 100MB each	$ 142.20
SiteGround	$ 3.95/month	Included	Unlimited email accounts. Shared 1000MB	$ 142.20

Appendix M.

Website Domain Name, Hosting, and Email

Bluehost - Domain registration, website hosting service, and email
Domain Name: rmibankingcomm.org
Associated Cost: $142.20/3 years

GoDaddy - Domain registration
Domain Name: rmifiu.org
Associated Cost: $12.17/year

Zoho Mail - Email
Associated Cost: Free, for up to 10 users

The following instructions were followed to link the rmifiu.org domain and Zoho Mail:
https://www.zoho.com/mail/help/adminconsole/godaddy.html

Common Email Tasks:

To add emails*:
*Note: Zoho free email plan has only 10 emails and Bluehost email only 5

Zoho Mail

1. Go to https://www.zoho.com/mail/login.html
2. Log in using your email and password (must be logging in as administration@rmifiu.org)
3. Hover over 'Control Panel' in the upper right corner until a drop down appears
4. Click on Mail & Docs
5. Click on User Details in the sidebar on the left
6. Click on 'Add User' in the menu bar along the top
7. Fill out the necessary information in the form

Bluehost

1. Go to https://my.bluehost.com/web-hosting/cplogin
2. Log in using your email and password (must be logging in as rmibankingcomm.org)
3. In the 'email' section, click 'Email Manager'
4. Under the 'email accounts' tab, click on 'create an email account'
5. Fill out the necessary information in the form

Appendix N.

Email Encryption using Outlook or Thunderbird:

To protect sensitive information, it is important that any email that you want to stay private is encrypted. To do this, it is recommended you use Outlook to encrypt and decrypt your messages. The following information is to help the Banking Commission and its financial entities set up and encrypt messages.

1. Getting a Digital Id

You must have a digital signature to sign every email you want to send encrypted. There are various sites, such as Comodo, that will give you are free email certificate. Ensure that you go to this site on Internet Explorer or Mozilla Firefox https://www.comodo.com/home/email-security/free-email-certificate.php
Follow the instructions to create and install your own security certificate.

2. Backing Up Digital Id

You must back up the digital signature somewhere on your computer for safe keeping and to install it into outlook/thunderbird. Follow the instructions here:
https://support.comodo.com/index.php?/Default/Knowledgebase/Article/View/71/18/how-do-i-backup-my-digital-id-certificate-windows-ie

3. Installing and Using your Secure Email Certificate with Outlook/Thunderbird

Follow these instructions to install the certificate into your email service provider. *Note
THUNDERBIRD: https://www.comodo.com/support/products/email_certs/thunderbird.php
OUTLOOK: start a new email and under Options, then Security Settings, check “Encrypt message” and “Add digital signature” and it may prompt you to click the document you want to sign with. You will need to import the document saved in the previous step.

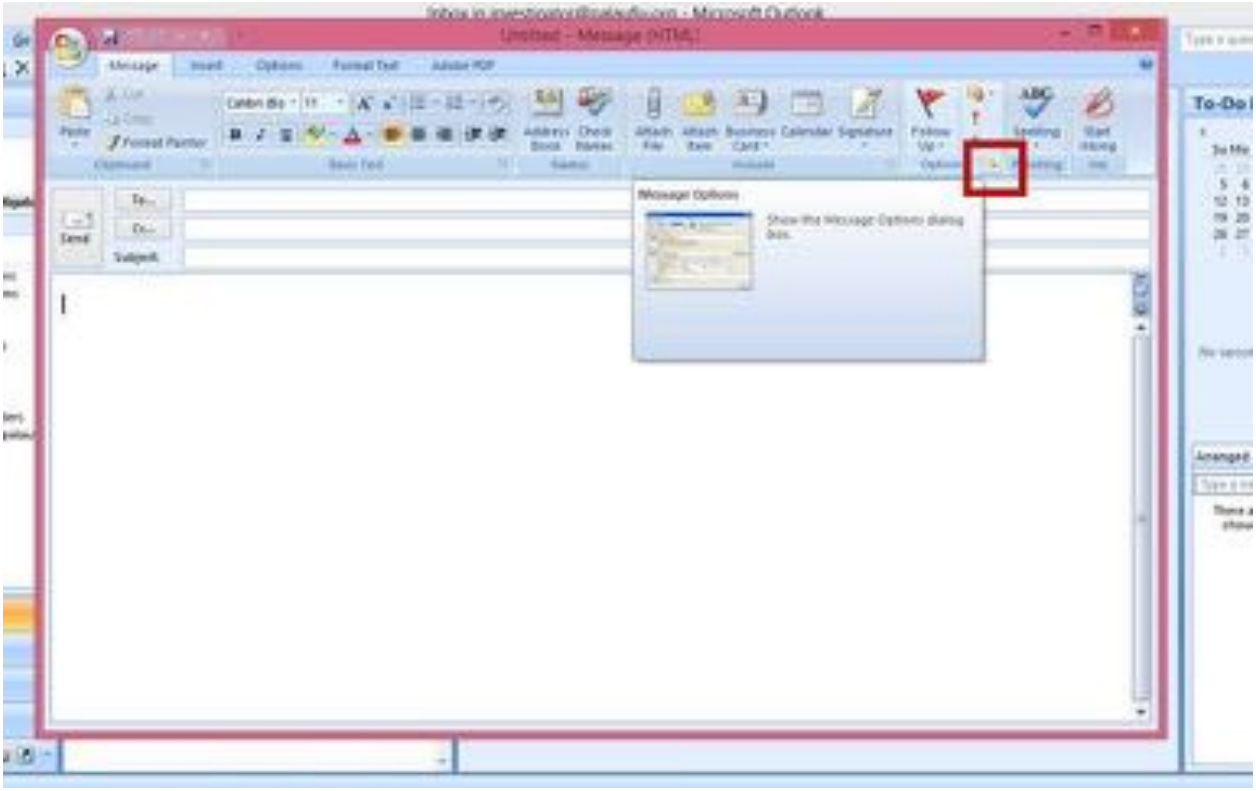
4. Exchanging Digital Signatures

When a message is encrypted, you need a way to decrypt it. The most common way of encrypting/decrypting messages is through public/private key encryption. A public key can only encrypt a message, not decrypt it. The only way to decrypt a message encrypted with that public key is to use the corresponding private key. This way, you can share your public key with anyone and everyone, and they can encrypt a message to you using your public key. Then you use your private key to decrypt it.
A digital signature includes your private key, and is also an assurance that it is you sending the message (not an imposter) and the contents haven’t been messed with. You can think of it like an old fashioned wax seal. To send encrypted messages to each other, you must send your digital signatures to each other, and save the key in your contacts.
You set up your digital signature one of two ways: you can send it on individual messages, or you can include it on all sent messages.

(You can also see these instructions here: https://support.office.com/en-za/article/Secure-messages-with-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6?ui=en-US&rs=en-ZA&ad=ZA)

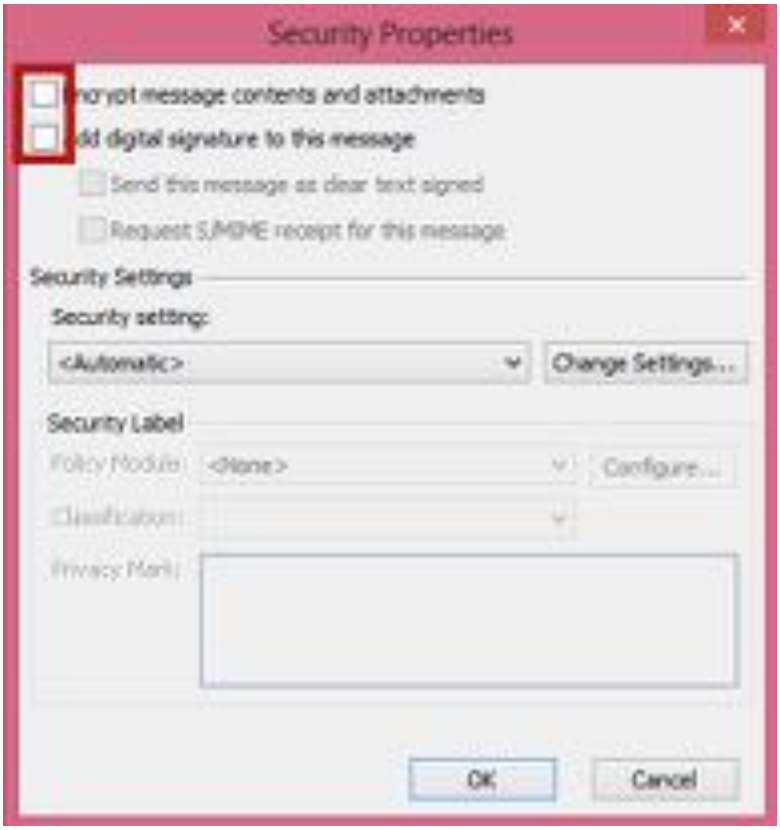
Digitally sign one message

1. When in the message, click the arrow under the 'Options' group



2. click on the 'Security Settings' button

3. Click on the checkbox next to ‘Add Digital Signature to this message’



4. click ‘OK’
5. compose and send your message as usual

Digitally sign all outgoing messages

1. Under the ‘Help’ Menu click ‘Privacy Options’
2. In the left side bar of the pop up box, click ‘Email security’
3. Under Encrypted e-mail, select the Add digital signature to outgoing messages check box.
4. If available, you can select one of the following options:

    a. If you want recipients who don't have S/MIME security to be able to read the message, select the Send clear text signed message when sending signed messages check box. This check box is selected by default.
    b. To verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered, as well as notification telling you who opened the message and when it was opened, select the Request S/MIME receipt for all S/MIME signed messages check box. When you send a message with an S/MIME return receipt request, this verification information is returned as a message sent to your Inbox.

5. Click OK.

Updating a contact to include their digital signature

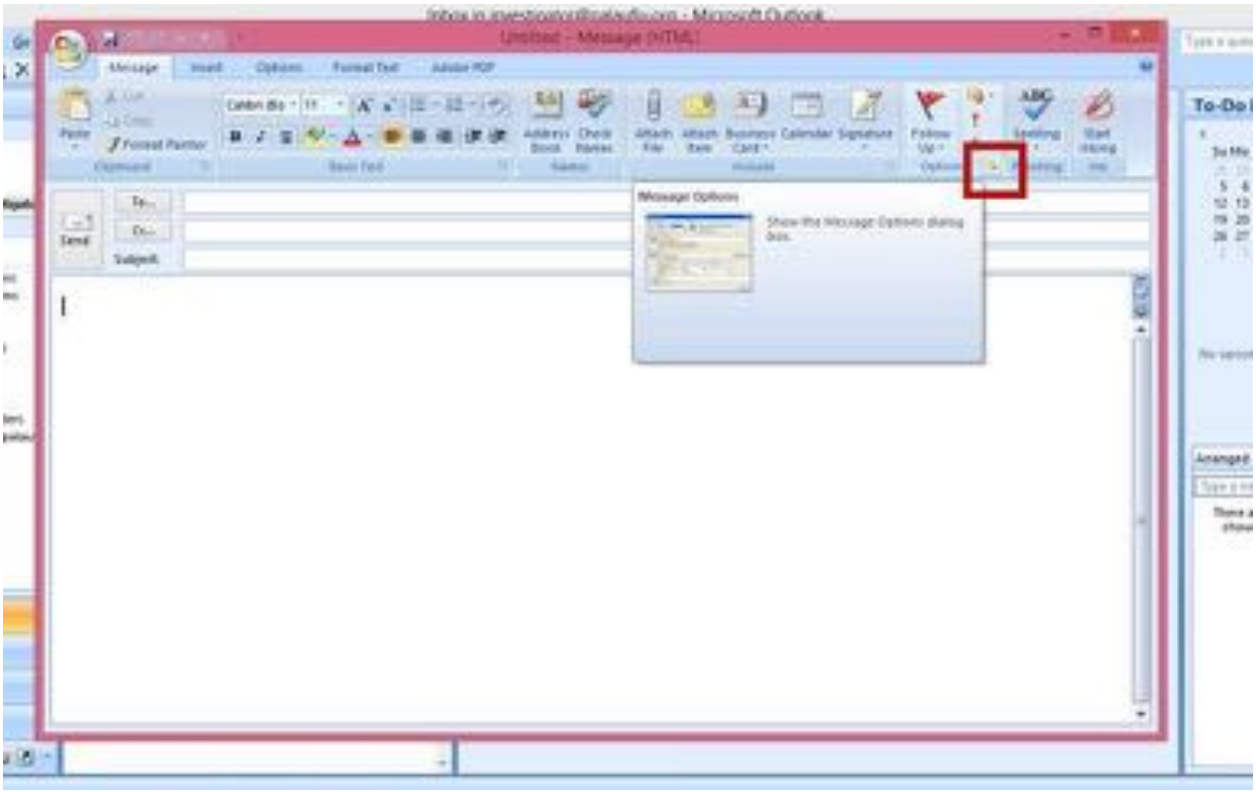
1. Right click on the email address in the header of the email
2. Click on ‘Update Contact’

Encrypting a Message

You have two options for encrypting messages, either encrypt them one at a time, or encrypt all outgoing messages. You can also read these steps here:
https://support.office.com/en-za/article/Encrypt-e-mail-messages-84d7e382-5f76-4d71-8705-324489b710a2

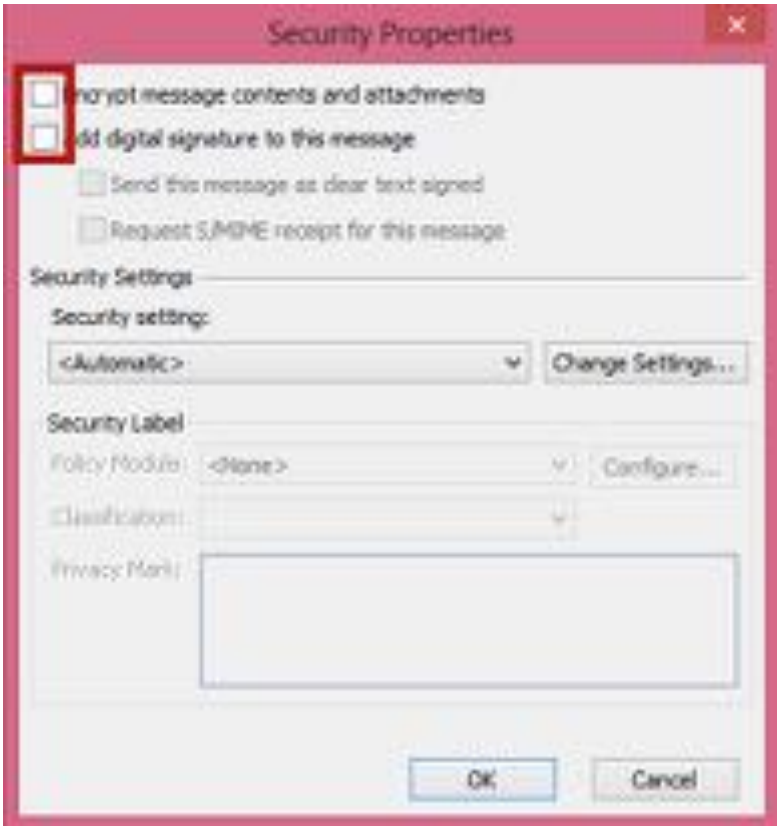
Encrypting a single message

1. When in the message, click the arrow under the ‘Options’ group



2. click on the ‘Security Settings’ button

3. Click on the checkbox next to ‘Encrypt message contents and attachments’



4. click ‘OK’
5. compose and send your message as usual

Encrypting all outgoing messages

1. On the Help menu, click privacy options, and then click E-mail Security.
2. Under Encrypted e-mail, select the Encrypt contents and attachments for outgoing messages check box.
3. Click OK.