Risk Assessment & Management in Merchant Capture Systems: A Threat Analysis Perspective

Kevin Streff
kevin.streff@dsu.edu

Sarin Shrestha
sshrestha17600@pluto.dsu.edu

Cody Delzer
cj.delzer@pluto.dsu.edu

College of Business & Information Systems
Dakota State University
Madison, SD 57042, USA

Abstract

Merchant Capture Systems (MCS) provide the ability to deposit checks remotely without visiting a brick-and-mortar bank. The adoption of this technology is increasing rapidly; however, security threats exist with merchant capture systems. This paper examined two prominent merchant capture architectures to determine and prioritize common security threats and mitigating controls. Threats were identified for three components of a typical merchant capture system: bank, merchant and technology service provider. The paper communicates common MCS threats and controls as gathered by a questionnaire, evaluated by security experts and verified by IT auditors and bank examiners. The study determined the likelihood and impact of each threat, calculated an asset threat score and an inherent risk score for a merchant capture system, and concluded data loss as the top security risks when checks are deposited remotely through a merchant capture system.

Keywords: Risk Assessment, Risk Management, Remote Deposit Capture (RDC), Merchant Capture System (MCS), Banking industry, and Security Threats.

1. INTRODUCTION

Remote Deposit Capture (RDC) emerged to automate the check deposit process, allowing business customers to remotely scan checks and transmit the scanned image to their financial institution without physically delivering the check to the depositary bank (Levitin, 2009). Merchant capture systems (MCS) are forecasted as a technology banks will most likely implement over the next several years, with an estimated 5 million capture points by 2014 (Meara, 2008) and 7.3 million users by 2015 (MarketsandMarkets, 2010).

The term "merchant" refers to business clients, such as the retailers, car dealers and other types of commercial clients, who desire remotely deposit checks without visiting the bank. Merchant capture systems appeared in the digital economy as a new method of providing commercial clients flexibility to deposit checks

from remote locations. For example, a Wal-Mart store may accept thousands of checks daily which need to get deposited as soon as possible. Wal-Mart would enjoy the benefits of no longer having to travel to the bank to deposit checks, reducing costs and floats. However, these efficiencies potentially expose banks to information security risks (McLaughlin, 2008).

The use of merchant capture became popular after the Check 21 Act was passed (Check21, 2003; Giudice & Johns, 2009) that mandated that digital checks become the legal equivalent to physical checks: that banks must accept a digital check just as they accept a paper check. MCS creates a digital image of the original check and sends the image to a financial institution for deposit via the Internet as an encrypted file (Fisher, 2009; Levitin, 2009).

Every financial institution must identify and mitigate the security and privacy issues before implementing MCS (FDIC, 2009). A comprehensive risk assessment is required to identify threats to MCS so management understands and addresses information risks. This paper examines MCS threats for three threat actors involved in a typical MCS: banks, merchants and technology service providers (TSP). Compensating controls are discussed to mitigate each identified threat.

2. ARCHITECTURES OF THE MERCHANT CAPTURE SYSTEMS

A MCS requires a PC, application software, an Internet connection, a check scanner and optionally a technology service provider. Scanners are typically sent to merchants via the postal service. Upon receipt, the merchant installs the scanner with telephone support. Yet other providers include the user manuals together with the scanners, so clients can install them (Valentine, 2008). Merchants will reserve a PC and load it with a MCS application that will process the deposit information. Based upon different types of MCS, these applications can be either software directly installed on their computers or website accessed designed to process depositing information.

Large banks typically develop their MCS solution while community banks generally license off-the-shelf solutions (Houseman & Nevle, 2009). The two common architectures of the MCS are: Merchant Capture with TSP and Merchant Capture without TSP.

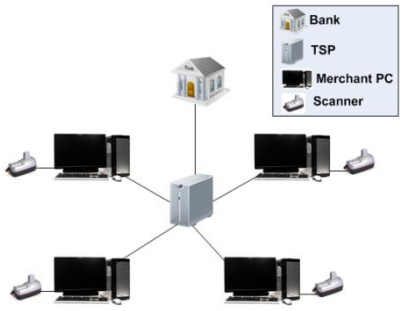

Figure 1: Merchant Capture System with TSP

Figure 1 demonstrates a typical MCS with a TSP. First, a merchant operator/employee scans the paper checks. As the checks are scanned, an image of each of check is generated and displayed on the PC, and the operator manually inputs the amount of money for each check. Alternatively, the PC may be provided with optical character recognition (OCR) software that is adapted to obtain the dollar amount of each check directly from the scanned image. In this case, the operator views the check images and verifies the amounts that are recognized by the OCR software. Once the images are created and the value of each check is obtained, the operator is asked to input the information including the account number of the client company to receive the deposit and some other information used to verify the sender's identity, such as the name of the operator, the company's address and the telephone number. The final step is a transfer of the data to the TSP's server, which analyzes the image quality of the scanned checks and forwards the deposit information through the Internet to the depository bank (Forth, Pierce, & Carey-Steckbaucer, 2007).

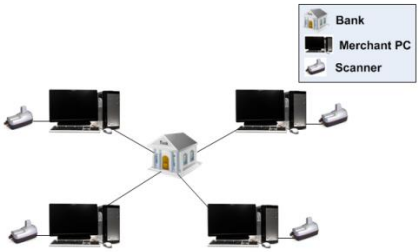

Figure 2: Merchant Capture System without TSP

Figure 2 illustrates a MCS without the service provider involved. Most of the detailed operational procedures remain the same as the former architecture; however, the deposit information from merchants is sent directly to the financial institution via the Internet.

3. LITERATURE REVIEW

Although remote deposit capture is a relatively new technology, remote banking can be traced decades back. Designed for serving customers without having to visit a bank personally, remote banking was initiated in the late 1960s with the introduction of an Automated Clearing House (ACH) system that made Electronic Funds Transfer (EFT) available. The first Automatic Teller Machine (ATM) was installed at a Chemical Bank in New York in 1969 (Bielski, 2008). ATMs introduced new conveniences, leading to a boom in ATM usage in banks, shopping malls, grocery stores, airports and other places of convenience. 403,000 ATMS were in use throughout the United States with average 239 new ATMs installed per day worldwide (Gammon, 2009).

Remote deposit platforms were extended to phone-based models in 1989 when First Direct, the first telephone based bank, was launched in the UK by HSBC bank (FinancialNews, 2008). This new concept of banking let the customers open accounts, make transactions, buy stocks and pay bills through their telephone system. Phone banking provided several advantages, including eliminating the cost of building new branches (Lennon, 1996).

Internet banking first appeared in the mid 1990s. Security First National Bank was the first bank offering Internet banking in 1995. Through the World Wide Web, customers browse their account information, carry out transactions and track payments on their PC. Internet banking was quickly offered by thousands of banks around the world by 1997. Today, most banks around the globe have a website to serve customers remotely through the Internet (Chou & Chou, 2000), yet few system include a remote deposit capability.

Mobile banking was conceptualized in the late 1990s to conduct banking commerce using mobile phones. However, technology concerns including screens which lacked the capability to show precise information, low-speed mobile phone networks, delayed adoption until 2000. With the advancement of high-speed networks for mobile phone, such as EDGE, GPRS, and 3G networks, mobile banking became practical (Riivari, 2005) to remotely deposit from a mobile platform.

To encourage innovation and efficiency in the payment system, Check Clearing for 21st Century Act (Check 21) became effective in 2004 (Check21, 2003; Jesus, 2006) to allow financial institutions to create, transmit, deposit and utilize an electronic image of the original check. Instead of transporting the original check to the bank, checks are cleared based upon a digital image. RDC models were introduced to scan and send electronic digital documents of deposit information from various remote locations (FDIC, 2009). When the digital documents are ready, they are sent to the financial institutions to complete the deposit process using specialized software (Fisher, 2009; Levitin, 2009).

According to the American Bankers Association (ABA) Banking Journal, merchant capture systems are very popular. Nearly 65% of American banks offer RDC; 58.5% of banks report that offering RDC does attract new business clients and 71.2% of banks state improved business client retention because of RDC (ABA, 2007, 2008). RDC customers are growing by 45 new customers per week, and more than 50% of the total commercial deposits are gathered through RDC (AmericanBanker, 2008). The number of scanners deployed for remote capture in the United States exceeded 700,000 scanners in 2011 (Meara, 2011). Celent's 2008 State of RDC report states two-thirds of U.S. banks have adopted the technology by the end of 2008 (Meara, 2008). Aite Group estimates that 350,000 accounts are enabled with RDC capability (Aite, 2010). Large banks leverage RDC to expand geographically, whereas small banks use RDC to substitute building physical branches (Ginovsky, 2008). Many credit unions utilize RDC to enhance their operational efficiency and reduce the courier costs of transporting paper check (Johnson, 2009). Bob Meara, a senior analyst in the banking group at Celent LLC, stated that, "In the history of U.S. financial services, there has never been a technology adopted faster than RDC" (Celent, 2008), with 7,100 financial institutions offering at least one commercial RDC solution by the end of 2011 (Chilingerian, 2011).

The Financial Crimes Enforcement Network identified 1,017 suspicious activity reports for violations pertaining to the remote capture (Bishop, 2011). American Banking Association's 2011 Deposit Account Fraud Survey estimated $893 million check related losses in 2010 (ABA, 2011). According to 2012 Faces of Fraud Survey, check fraud is listed in the top security threat (BankInfoSecurity, 2012). These

circumstances support the need to risk assess and manage MCS at every bank.

4. RISK ASSESSMENT AND MANAGEMENT

Security risk management is a continuing process of identifying and prioritizing risks to minimize, monitor and control the probability and impact of unfortunate events (Spears & Barki, 2010). Various risk assessment models have been proposed. National Institute of Standards and Technology (NIST, 2010) proposed a framework in NIST SP 800-37 to improve the information security posture, and reinforce risk assessment processes to encourage cooperation among federal organizations. Saleh, Refai, and Mashhour (2011) proposed a risk assessment framework that discovers system's threats and vulnerabilities.

Similarly, numerous information security standards and guidelines have been proposed and developed to protect information assets. Gramm Leach Bliley Act is a federal law for financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity and confidentiality of information (FDIC, 2001; GLBA, 1999). Generally Accepted System Security Principles is a mutual effort to develop and maintain a set of rules, practices, and procedures to achieve information confidentiality, integrity, and availability between international countries, unifying and intensifying upon existing authoritative sources (Grimaila & Kim, 2001; Poore, 1999). The Federal Information Processing Standards is issued by the National Institute of Standards and Technology (NIST) to provide mandatory guidelines such as for security and interoperability for government agencies (FIPSPUBS, 1996).

Innovative models have been explored and deployed; however, due to the number of calculations that are performed when conducting a risk assessment, it is common for banks to employ a one-to-one-to-one or one-to-one-to-few method, which leads to the assumption that one asset has one threat and that one threat has either one or a few controls to mitigate the risk imposed by the threat. However, a systematic and accurate risk assessment method uses a one-to-many-to-many approach. This method assumes that each asset has many threats, and each of those threats has many controls to mitigate the risk.

Podhradsky, Streff, Pauli, and Engebretson (2011) conceptualized an automated risk assessment model which allows a bank to complete comprehensive and thorough one-to-many-to-many risk assessments. This method would define generic assets, each with a unique protection profile. The method would allow banks to develop protection profiles based upon the confidentiality (C), integrity (I), availability (A), and volume (V) of data each asset processes, stores, and transmits; identify threats based upon their impact and likelihood; apply controls, and generate risk reports. When the remote deposit is considered, the bank also has to focus on technology controls, such as network security settings, controls over the transaction, encryption, and physical security controls (Joseph, 2011).

5. RESEARCH METHODOLOGY

In this study, merchant capture systems were studied to understand protection profiles, threats and mitigating controls. Regarding protection profiles, the study leveraged the Podhradsky et al. (2011) approach and assigned the merchant capture system asset a protection profile (APP) based upon a high, medium, or low categorization. These qualitative ratings are turned into quantitative ratings of 3, 2, and 1 respectively. Hence, the asset MCS has been assigned an Asset Protection Profile rating of 9 of high confidentiality, high integrity, medium availability and low volume.

Confidentiality (C)	High	3
Integrity (I)	High	3
Availability (A)	Medium	2
Volume (V)	Low	1
Asset Protection Profile (APP)		**9**

Table 1: MCS Asset Protection Profile

High confidentiality as information is sensitive; its disclosure would violate federal banking regulations and/or result in significant harm to the institution. High integrity as accuracy of the information is critical; its modification or incorrectness would cause significant issues. Information availability is of moderate concern; recovery must be made within few days. Volume is rated low as only a small amount of information is regularly stored, processed, or

transmitted using merchant capture systems. The CIA-V rankings are described further in Table 6 of the Appendix.

The research team developed a model that allows for reliable risk assessment improvement through identification of threats, and a process for verification and adjustments to the formerly identified threats. The major components in this process include:

- Researchers (One Professor and two Graduate Assistants).
- Security Consultants (content team composed of four InfoSec consultants who generate MCS risk assessment based upon results of the Survey Questionnaire).
- Risk Assessment Database (Captured research results for MCS threats and controls).
- Third-party IT auditors (Audit the MCS risk assessment and provide feedback).
- Bank Examiners (Examine the MCS risk assessment and MCS audit to provide feedback).

The complete process consists of seven steps is illustrated in Figure 3.

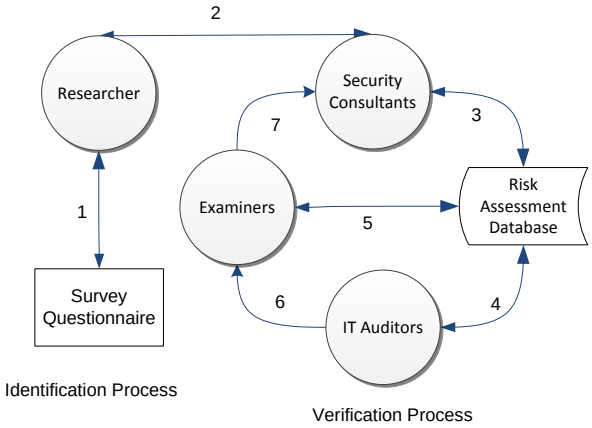

Figure 3: Research Methodology

The methodology can be sub-divided into two separate sub-processes: Identification and Verification. Identification is the process where researchers ask MCS users and experts what they believe the typical threats and controls are for merchant capture systems. Verification is the process where researchers refine the data gathered during Identification to improve the quality of the data.

Identification: The sub-process on the left of Figure 3 is intended to be a process of threat identification and initiates with Researchers collecting data from survey questionnaire that identify potential threats to MCS systems. The questionnaire was distributed among 125 individuals who were exposed in this MCS processes. Among them, 98 responses were collected. These individuals were bankers, merchant operators, and information security officers who completed the survey individually and the results were tabulated. The threats were listed with the columns of impact and likelihood with the basic rating of high, medium and low in the table for all three actors. The survey questionnaire is shown in Appendix.

Verification: After Identification is complete, a group of security consultants conducts a MCS IT Risk Assessment and provides the results in the Risk Assessment Database. The security consultants used the data collected via the survey questionnaire to develop the MCS risk assessment in ten banks. Next, a group of IT Auditors reviewed the data inserted by security consultants and provide their own recommendations to threats identified and Asset Protection Profiles and inserted the refined data into the Risk Assessment Database. Finally, a group of bank examiners, who identify improvement opportunities for risk assessment, examines the data and provide their own perspectives to identified threats and Asset Protection Profiles and inserted the data into the Risk Assessment Database. The process completes its first iteration with step 7, when the group of security consultants review findings and recommendations from independent third party IT auditors, and finally return with that information to step 3 where the process of improvement continues to cycle, ensuring the Risk Assessment database remains accurate and relevant.

Each threat is assigned a threat score called Asset Threat Score (ATS) based on its Impact (I) and Likelihood (L). Impact is the estimated degree of loss or damage to the asset or institution and assigned a value between 1 and 3 with 1 representing little or no impact and 3 representing devastating impact. Likelihood is the estimated degree of possibility the threat may have an impact on the organization in a given time and assigned a value between 1 and 3 with 3 representing that it is highly likely that a threat will occur and 1 vice-versa. The impact and likelihood rating for each threat is multiplied to produce an Asset Threat Score. Finally, the Total Asset Threat Score (TATS) is equal to the sum of all asset threat scores and the Asset Inherent Risk Score (AIRS) is calculated by taking the Asset Total Threat Score times the

Asset Protection Profile. These concepts are defined in Table 5 in Appendix.

6. RESULTS AND DISCUSSIONS

Using the methodology described above, the top MCS critical threats are described for banks, merchants, and service providers.

MCS Critical Threats for Banks

Data Loss

Data loss is the insider risk of stealing or providing unauthorized access to sensitive information. Data Loss Prevention (DLP) systems have become common place in large banks while small and medium-sized banks generally find them unaffordable. Other solutions to prevent data loss include employee operational and security training, and well-composed security policies and procedures.

Unauthorized Access

Unauthorized physical and system access are significant risks to the bank in MCS. By the physical method, the attacker can steal or sabotage the bank's physical assets in the MCS while by the system method, the attacker can steal or delete the information in the MCS. If the attacker gains access to the administrator account, he/she can change the security settings in order to install malicious software that creates backdoor to the system. Although the impact of unauthorized access is obviously high, likelihood of occurrence remains medium for each of the methods since the bank usually has sound physical security considerations.

Outsourced

According to statistics from the ABA Journal, half of the banks among the U.S. choose outsourced solutions (ABA, 2007). It is true that having a third party involved in the process of MCS can remove many burdens from the bank, such as MCS infrastructure development, signing multiple sourcing contracts, updating and maintaining the software and hardware, and customer trainings (Houseman & Nevle, 2009). However, a new threat called outsourced is generated under the situation. This threat can be mitigated by performing due diligence in selecting service providers; it still has high impact.

MCS Critical Threats for Merchants

The most critical threats to merchants are found in Table 3. These threats are related in that they are associated with people. Some of them including data loss, unauthorized physical, and system access have already been described from the perspective of bank. Threats like social engineering and intentional misuse demonstrate that people the most risky part for the merchant. Unlike employees from banks paid by monthly salaries, many small business employees are seasonal or hourly. The requirement of the educational background at a merchant site is likely less than the educational requirement at a bank. Most of the merchant companies would not do employee background checking since they are hiring part-timers. The low education requirement and the lack of employee background checking leave the potential that people with a criminal background or poor credit histories might get the job which increases the probability of high intentional misuse.

	Bank		
Threats	I	P	I*P
Data Loss	H	M	6
Outsourced	H	M	6
Unauthorized Physical Access	H	M	6
Unauthorized System Access	H	M	6
Degraded/ Unavailable	M	M	4
Eavesdropping/ Sniffing	M	M	4
Hardware Failure	M	M	4
Intentional Misuse	M	M	4
Malicious Software	M	M	4
User Error	M	M	4
Unauthorized Remote Access	H	L	3
Environmental Incident	M	L	2
Man-made/ Natural Disaster	M	L	2
Software Acquisition	M	L	2
Social Engineering	M	L	2
Unauthorized Viewing	L	L	1
Total Asset Threat Score			**60**
Asset Inherent Risk Score			**540**
Legend:			
"I"—Impact; "P"—Likelihood; "; "H"—High; "M"—Medium; "L"—Low			
Value:			
High = 3; Medium = 2; Low = 1			

Table 2: Bank MCS Threats

	Merchant		
Threats	I	P	I*P
Unauthorized Physical Access	H	H	9
Data Loss	M	H	6
Intentional Misuse	M	H	6
Social Engineering	M	H	6
Unauthorized System Access	M	H	6
Eavesdropping/ Sniffing	M	M	4
User Error	M	M	4
Malicious Software	H	L	3
Degraded/Unavailable	L	M	2
Hardware Failure	L	M	2
Environmental Incident	L	L	1
Man-made/ Natural Disaster	L	L	1
Unauthorized Viewing	L	L	1
Total Asset Threat Score			**51**
Asset Inherent Risk Score			**459**
Legend:			
"I"—Impact; "P"—Likelihood; "; "H"—High; "M"—Medium; "L"—Low			
Value:			
High = 3; Medium = 2; Low = 1			

Table 3: Merchants MCS Threats

Most of the merchant companies do not have security policies, procedures and do not offer security training. The consequence is increasing the probability of data loss and social engineering. In addition, not all merchants employ layered security like a bank, which means assets like checks, computers, and scanners are not hard to access by criminals.

MCS Critical Threats for TSPs

In MCS, a TSP typically deals with providing software and hardware, customer training, system maintenance, and data manipulating, which includes gathering data from the merchant then transferring it to the bank. The data from merchants being transferred to the TSP is considered sensitive, due to the data containing the image of the scanned checks to be deposited. Given this fact, data loss is possible for the employees of the TSP, who have access to the data, either by unintentionally exposing the data to the public or deliberately selling it. Although, a data breach from insiders can be mitigated by employee training and background checking, there are still many external attackers targeting TSPs.

MCS threats for the TSP include:

	Third Party		
Threats	I	P	I*P
Data Loss	H	H	9
Malicious Software	H	H	9
Social Engineering	H	H	9
Unauthorized System Access	H	M	6
Degraded/ Unavailable	M	M	4
Eavesdropping/ Sniffing	M	M	4
Hardware Failure	M	M	4
Intentional Misuse	M	M	4
Unauthorized Physical Access	M	M	4
Environmental Incident	M	L	2
User Error	M	L	2
Man-made/ Natural Disaster	M	L	2
Software Acquisition	M	L	2
Unauthorized Remote Access	M	L	2
Unauthorized Viewing	L	L	1
Total Asset Threat Score			**64**
Asset Inherent Risk Score			**576**
Legend:			
"I"—Impact; "P"—Likelihood; "; "H"—High; "M"—Medium; "L"—Low			
Value:			
High = 3; Medium = 2; Low = 1			

Table 4: TSP MCS Threats

Malicious software like Trojan horses and backdoors are good weapons for attackers to gain access to data from the computer systems of the TSP. Combined with a little social engineering like email spam, malicious software can be installed on the system by innocent employees who fall into the trap. Another option an attacker may use is to hire someone from the TSP to install the software directly onto the system. Therefore, data loss, malicious software, and social engineering are the three most critical threats for the TSPs.

Top MCS Critical Threats for Banks, Merchants and TSP

The summary of critical threats to the Bank, Merchant and Third Party is in Table 7 in Appendix. The top five MCS critical threats are identified for banks, merchants, and service providers are as:

Data Loss
As one of the most critical threats, data loss can be described as someone intentionally or unintentionally releasing information to unauthorized recipients. The threat can be conducted either by not-well trained or by disgruntled employees through sending sensitive information of the company to unauthorized individuals or posting the information directly on the Internet. In March 2010, a former employee with TD Bank releases the customer information to accomplices who withdrew more than $200,000 from 13 bank customer accounts (Patel, 2010).

Malicious Software
It is a program that performs unauthorized processes that will lead to a malicious impact on the information systems confidentiality, integrity and availability. Symantec Corporation discovered more than 240 million distinct new malicious programs in 2009, a 100% increase over 2008 (Symantec, 2009).

Social Engineering
Rather than using complex computer techniques to gather information from the target system, social engineering is an attack based on deceiving users or administrators by an unauthorized person masquerading as a rightful user. This attack is usually performed in an attempt to gain illicit access to systems or confidential information. A mobile banking application on Android platform in December 2009 caused more than 50 fraudulent banking applications to appear (Patel, 2010). These applications attempted users to enter their bank account numbers, password and other personal information.

Unauthorized Physical Access
It is defined as someone intentionally infiltrating a secure area. It can be exploited by external attackers or internal disgruntled employees. The consequences of the threat range from theft, sabotage, even to unauthorized system access.

Unauthorized System Access
It is gaining unauthorized access to a system by physically interacting with it. The example of exploiting this threat is where an unauthorized individual or an attacker logs into the system with stolen credentials or bypassing security through hardware using CD drives and USB ports.

Top MCS Controls for Threats Identified for Banks, Merchants and TSPs
The financial institution should assess potential risks and regulatory constraints under Bank Secrecy Act when implementing MCS (FDIC, 2009). There is a healthy relationship between financial institutions and a payment processor. A payment processor is a customer who deposits checks and process payments for third party merchant clients (FDIC, 2012). Usually, payment processors effects legal payment transaction for merchant clients, the risk profile can deviate depending on the customer type. For instance, payment processors that deal with online clients may have a high risk-profile as they have the tendency to display a higher prevalence of illegal activities or fraud when compare to other businesses. Financial organization should comprehend, authenticate, and examine the activities and the entities associated to the account relationship and also outline the comprehensible lines of responsibility for governing risks related with the payment processor relationships (FDIC, 2012). The control for mitigation includes inspection and monitoring of accounts for suspicious activity, enhanced due diligence and consumer complaints. Implementing proper countermeasure may facilitate to discover payment processors that process items for fraudulent or unscrupulous merchants. To limit the potential risk associated, the financial institutions should implement risk mitigation policies including appropriate controls for the risk and procedures designed to reduce the probability of unauthorized transactions used by unscrupulous merchants.

Top controls to mitigate those threats include:

Controls for Threat- Data Loss
i. Security Information and Event Management: An application that collects, stores and analyzes security log data from multiple systems for data retention and detection of unauthorized activity.
ii. Unique User Accounts: The process of assigning unique usernames that allow them to distinguish from each other and prevent them from being guessed easily.
iii. User Activity Logs: Logs used to track details about transactions and events performed by a user.
iv. Administrator Activity Logs: Logs used to track details about transactions and events performed by an administrator.
v. Data Loss Prevention: A tool that actively monitors, blocks, and reports on data leaving

the Bank to ensure sensitive information is not transmitted to unauthorized parties. Data is allowed or blocked based on the analysis of its content, instead of its source or other criteria.

Controls for Threat- Unauthorized Physical Access
i. Remote Capture User Security Controls Audit: Performing a review of the remote user's security controls to ensure the system is sufficiently protected.
Examples of a Remote Capture User Security Controls Audit are On-site, Self-Assessments, Independent Reviews, etc.
ii. Restricted Access Area: A secured area accessible only by authorized personnel or by those granted temporary access.
iii. Surveillance Cameras: Cameras that provide archived surveillance for an area.
iv. Monitored Location: Locating an asset where it will be visible by an employee who is responsible for its physical security.
v. Motion Detection: A system that triggers an alarm or other event when it detects motion.

Controls for Threat- Unauthorized System Access
i. Security Information and Event Management
ii. Remote Capture User Security Controls Audit
iii. Unique User Accounts
iv. User Activity Logs
v. Firewall -Ingress Filtering: A dedicated appliance or software running on individual computers that inspects network traffic passing into the network and denies or permits passage based on a set of rules.

Controls for threat- Social Engineering
i. Data Loss Prevention
ii. Incident Response Program: Actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies. The goal of an incident response program is to minimize damage to the institution and to its customers through intrusion containment and the restoration of systems.
iii. Inactive Lockout: Locking a user's session after a specified period of inactivity.
iv. Website Filtering: Prevents computer users from viewing inappropriate or unauthorized websites.
v. Social Engineering Security Awareness: Educating employees on identifying and preventing social engineering attempts.

Controls for threat- Malicious Software
i. Security Information and Event Management
ii. Firewall -Ingress Filtering
iii. Intrusion Detection / Prevention: A security management system to identify and prevent possible security breaches, which include both intrusions (attacks from outside) and misuse (attacks from within).
iv. Back-up Critical Data: Completing regularly scheduled backups of critical information.
v. Formal Patching Process: A defined process for identifying missing updates and patches and deploying them on a scheduled basis or immediately if needed.

Table 8 in Appendix illustrates the top five controls for each identified threat above.

7. CONCLUSION

The adoption of Merchant Capture System poses challenges and security threats to financial institutions. Hence, prior implementing this model, a risk assessment should be performed to identify risk and security threats. The paper identifies the most common threats and controls for MCS to support the risk assessment process at a bank. Management should also ensure the appropriate policies and controls are in place to mitigate those threats including physical and logical access controls over Merchant Capture System.

8. REFERENCES

ABA. (2007). Remote Deposit Capture: Bucks into bits begins to bite. *ABA Banking Journal, 99*(3), S4-S6.

ABA. (2008). Remote Deposit Capture: Making The Promise Pay Off. *ABA Banking Journal, 100*(3), S11-S18.

ABA. (2011). 2011 Deposit Account Fraud Survey: American Banking Association.

Aite. (2010). Remote Deposit Capture Risk Management: Raising the Bar (Vol. 166): Aite Group.

AmericanBanker. (2008). Remote Deposit Capture Partnership for Success. *American Banker Magazine, 118,* 11.

BankInfoSecurity. (2012). 2012 Faces of Fraud survey. BankInfoSecurity: Information Security Media Group.

Bielski, L. (2008). Eight Tech Innovations that took banking into the 21st Century. *ABA Banking Journal, 100*(11), 84-89.

Bishop, B. (2011). The SAR Activity Review - Trends Tips & Reviews (Vol. 20, pp. 1-94). http://www.fincen.gov/news_room/rp/files/sar_tti_20.pdf: Financial Crimes Enforcement Network.

Celent. (2008). Remote deposit capture carries risk as well as convenience. In M. Savage (Ed.).

Check21. (2003). Public Law 108-100: An Act (pp. 117). 108th Congress.

Chilingerian, N. (2011). RDC Reaches Adoption Plateau *Issue of Credit Union Times*: Celent.

Chou, D. C., & Chou, A. Y. (2000). A Guide to the Internet Revolution in Banking. *Information Systems Management, 17*(2), 51.

FDIC. (2001). Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information.

FDIC. (2009). Risk Management of Remote Deposit Capture from http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf

FDIC. (2012). Payment Processor Relationships Revised Guidance: Federal Deposit Insurance Corporation.

FinancialNews. (2008). History of the First Direct Bank

FIPSPUBS. (1996). Federal Information Processing Standards Publications Retrieved 04/07, 2013, from http://www.itl.nist.gov/fipspubs/geninfo.htm

Fisher, D. M. (2009). Exam Council spells out remote capture risks. *ABA Banking Journal, 101*(3), 34-35.

Forth, T. J., Pierce, J. D., & Carey-Steckbaucer, H. (2007). USA Patent No. 20070086642. P. B. Inc.

Gammon, K. (2009). ATMs by the Numbers. *Wired Magazine*.

Ginovsky, J. (2008). Reviving up for Remote Deposit Capture. *Community Banker, 17*(9), 28-30.

Giudice, E. L. D., & Johns, N. Z. (2009). Risk Management for Remote Deposit Capture. *Bank Accounting & Finance, 22*(3), 39-41.

GLBA. (1999). Public Law 106-102: Gramm–Leach–Bliley Act (pp. 143). 106th Congress.

Grimaila, M. R., & Kim, I. (2001). An undergraduate business information security course and laboratory. *Journal of Information Systems Education, 13*(3), 189-195.

Houseman, K., & Nevle, M. (2009). Financial Institutions Must Rethink Their Remote Deposit Capture Support Models (pp. 1-9): First Data Corporation.

Jesus, A. D. (2006). Remote Deposit Capture – A Practical Guide for Corporations. 1-20.

Johnson, T. (2009). Remote Deposit Capture. *Credit Union Management, 32*(2), 22-25.

Joseph, C. (2011). Understanding and Addressing Risk of Merchant Capture (pp. 16-17). West Virginia.

Lennon, D. (1996). Tele-banking. *Europe*(359), 38.

Levitin, A. J. (2009). REMOTE DEPOSIT CAPTURE: A LEGAL AND TRANSACTIONAL OVERVIEW. *Banking Law Journal, 126*(2), 115-122.

MarketsandMarkets. (2010). A New Look at Merchant Remote Deposit Capture (pp. 1-82). Markets and Markets.

McLaughlin, S. (2008). How & Why to Implement a Remote Deposit Capture Program. *The RMA Journal, 90*(7), 22-24.

Meara, B. (2008). State of Remote Deposit Capture 2008: Sprint Becomes a Marathon (pp. 49): Celent.

Meara, B. (2011). State of Remote Deposit Capture 2011: Signs of a Maturing Market: Celent.

NIST. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach *Information Security* (pp. 1-93): National Institute of Science and Technology.

Patel, R. (2010). Cybercrime: How to Protect Your Financial Institution. *Michigan Banker, 22*.

Podhradsky, A., Streff, K., Pauli, J., & Engebretson, P. (2011). *Restructured Information Technology Risk Assessment Model for Small and Medium-sized Financial Institutions*. Paper presented at the Proceedings of the 11th Annual Hawaii International Conference on Business, Honolulu, HI, USA, May, 2011.

Poore, R. S. (1999). Generally Accepted System Security Principles. *Information Systems Security, 8*(3), 27-77.

Riivari, J. (2005). Mobile Banking: A powerful new marketing and CRM tool for financial services companies all over Europe. *Journal of Financial Serivces Marketing, 10*(1), 11-20.

Saleh, Z. I., Refai, H., & Mashhour, A. (2011). Proposed Framework for Security Risk Assessment. *Journal of Information Security, 2*, 85-90.

Spears, J. L., & Barki, H. (2010). USER PARTICIPATION IN INFORMATION SYSTEMS SECURITY RISK MANAGEMENT. *MIS Quarterly, 34*(3), 503-522.

Symantec. (2009). Internet Security Threat Report (Vol. XV): Symantec Corporation.

Valentine, L. (2008). The RDC experience: Captivating. *ABA Banking Journal, 100*(3), 36-40.

Appendices and Annexures

Concepts	Definitions
Confidentiality (C)	Confidentiality is the processes, policies, and controls employed to protect information against unauthorized access or use
Integrity (I)	Integrity is the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner that compromise accuracy, completeness, and reliability
Availability (A)	Availability is the processes, policies, and controls used to ensure authorized users have prompt access to information, protecting against intentional or accidental attempts, to deny legitimate users access to information or systems
Volume (V)	Volume is the amount of information stored, processed, and transacted by an asset
Asset Protection Profile (APP)	Asset Protection Profile is a score calculated by adding the quantitative score for confidentiality, integrity, availability and volume for the asset
Asset Threat Score (ATS)	Asset Threat Score is a score calculated by the multiplication of Impact (I) and Likelihood (P) rating for each threat of the asset
Total Asset Threat Score (TATS)	Total Asset Threat Score is equal to the sum of all threat scores
Asset Inherent Risk Score (AIRS)	Asset Inherent Risk Score is a score calculated by taking the Total Threat Score times the Asset Protection Profile for the asset

Table 5: List of Concepts with the Definitions

Confidentiality	**High:** Information is sensitive; its disclosure would violate federal banking regulations and/or result in significant harm to the institution. **Medium:** Information is considered internal; its disclosure may violate federal banking regulations and/or result in moderate harm to the institution. **Low:** Information is for public consumption; its compromise would not be harmful to the institution.
Integrity	**High:** Accuracy of the information is critical; its modification or incorrectness would cause significant issues. **Medium:** Accuracy of the information is important, but not absolutely critical; its modification or incorrectness may cause moderate issues. **Low:** Accuracy of the information is of low concern; its modification or incorrectness may be inconvenient but could likely go unnoticed and cause few issues to the institution.
Availability	**High:** Information availability is of significant concern; recovery must be made within 24 hours. **Medium:** Information availability is of moderate concern; recovery must be made within 1 week. **Low:** Information is readily available elsewhere; recovery within 30 days is satisfactory.
Volume	**High:** There is a large amount of data regularly stored, processed, or transmitted. **Medium:** A moderate amount of information is regularly stored, processed, or transmitted. **Low:** Only a small amount of information is regularly stored, processed, or transmitted.

Table 6: CIA-V Rankings

	Bank			Merchant			TSP			
Threats	I	P	I*P	I	P	I*P	I	P	I*P	Total
Data Loss	H	M	6	M	H	6	H	H	9	21
Unauthorized Physical Access	H	M	6	H	H	9	M	M	4	19
Unauthorized System Access	H	M	6	M	H	6	H	M	6	18
Social Engineering	M	L	2	M	H	6	H	H	9	17
Malicious Software	M	M	4	H	L	3	H	H	9	16
Intentional Misuse	M	M	4	M	H	6	M	M	4	14
Eavesdropping/ Sniffing	M	M	4	M	M	4	M	M	4	12
Degraded/ Unavailable	M	M	4	L	M	2	M	M	4	10
Hardware Failure	M	M	4	L	M	2	M	M	4	10
User Error	M	M	4	M	M	4	M	L	2	10
Outsourced	H	M	6	-	-	-	-	-	-	6
Environmental Incident	M	L	2	L	L	1	M	L	2	5
Man-made/ Natural Disaster	M	L	2	L	L	1	M	L	2	5
Unauthorized Remote Access	H	L	3	-	-	-	M	L	2	5
Software Acquisition	M	L	2	-	-	-	M	L	2	4
Unauthorized Viewing	L	L	1	L	L	1	L	L	1	3
Total Asset Threat Score			**60**			**51**			**64**	**175**
Asset Inherent Risk Score			**540**			**459**			**576**	**1575**
Legend:										
"I"—Impact; "P"—Likelihood; "H"—High; "M"—Medium; "L"—Low										
Value:										
High = 3; Medium = 2; Low = 1										

Table 7: Threats of Merchant Capture Systems

	Five Controls for each Threat				
Threats	**Control 1**	**Control 2**	**Control 3**	**Control 4**	**Control 5**
Data Loss	Security Information & Event Management	Unique User Accounts	User Activity Logs	Administrator Activity Logs	Data Loss Prevention
Unauthorized Physical Access	Remote Capture User Security Controls Audit	Restricted Access Area	Surveillance Cameras	Monitored Location	Motion Detection
Unauthorized System Access	Security Information & Event Management	Unique User Accounts	User Activity Logs	Administrator Activity Logs	Firewall- Ingress Filtering
Social Engineering	Data Loss Prevention	Incident Response Program	Inactive Lockout	Website Filtering	Social Engineering Security Awareness
Malicious Software	Security Information & Event Management	Firewall-Ingress Filtering	Intrusion Detection / Prevention	Back-up Critical Data	Formal Patching Process
Intentional Misuse	Security Information & Event Management	Remote Capture User Security Controls Audit	Unique User Accounts	User Activity Logs	User Privileges & Restrictions
Eavesdropping/ Sniffing	Security Information & Event Management	Intrusion Detection / Prevention	Malware Protection	Encrypt Transmitted Data	----------

Degraded/ Unavailable	Firewall- Ingress Filtering	Firewall- Egress Filtering	Incident Response Program	Back-up Critical Data	Formal Patching Process
Hardware Failure	Back-up Critical Data	Backup Recovery Test	Hardware Health Monitor	Power Conditioning	RAID
User Error	Security Information & Event Management	User Activity Logs	User Privileges & Restrictions	Administrator Activity Logs	Data Loss Prevention
Outsourced	Business Continuity Plan	Formal Third Party Selection	Formal Third Party Review	Business Continuity Plan Test	Escrow
Environmental Incident	Secure Equipment & Capable Placement	Temperature Control	Humidity Control	Environment Monitor	Food & Liquid Filtering
Man-made/ Natural Disaster	Back-up Critical Data	Backup Recovery Test	Business Continuity Plan	Business Continuity Plan Test	Redundancy/Contingency Agreement
Unauthorized Remote Access	Security Information & Event Management	Remote Capture User Security Controls Audit	Unique User Accounts	User Activity Logs	Firewall- Ingress Filtering
Software Acquisition	Business Continuity Plan	Formal Third Party Selection	Formal Third Party Review	Business Continuity Plan Test	Escrow
Unauthorized Viewing	Remote Capture User Security Controls Audit	Inactive Lockout	Monitor Placement	Privacy Filter	Clear Screen Awareness

Table 8: Top Five Controls for Threats in Merchant Capture Systems

User Questionnaire: Impacts and Likelihood of Threats

The questionnaire requests you to evaluate the likelihood and impacts of each threat provided to you by our Expert Group arranged in alphabetical order. There are no right/wrong answers. It is very important that honest evaluations are indicated.

Please choose "H", "M" or "L" for High, Medium, and Low respectively for the likelihood (P) and impact (I) for the following identified threats for three actors: bank, merchant and technology service provider as third party.

	Bank		**Merchant**		**Third Party**	
Threats	Impact (I)	Likelihood (P)	Impact (I)	Likelihood (P)	Impact (I)	Likelihood (P)
Data Loss	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Degraded / Unavailable	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Eavesdropping / Sniffing	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Environmental Incident	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Hardware Failure	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Intentional Misuse	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Malicious Software	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Man-made / Natural Disaster	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Outsourced	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L

Social Engineering	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Software Acquisition	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Unauthorized Physical Access	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Unauthorized Remote Access	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Unauthorized System Access	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
Unauthorized Viewing	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L
User Error	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L	☐ H ☐ M ☐ L