New Guidance and New Challenges in Remote Payment Systems

Thomas Hinkel, Director of Compliance

INTRODUCTION

Recent FFIEC guidance on Retail Payment Systems[1] has increased the focus on electronic transactions and payment methods. If your financial institution is offering any products or services with "remote" in the name, this guidance will affect you. However, simply being compliant with the current guidance may address the regulatory risks of these products, but not go far enough to actually prevent fraud and the corresponding financial and reputational losses. Similarly, relying solely on the security mechanisms of your product doesn't fully address the risks either.

BACKGROUND

Although paper checks remain the most popular payment vehicle, electronic payment methods are becoming more popular. In fact…

> *"…in an increasing number of payment situations, checks are no longer the most convenient payment instruments for consumers, or the most cost-effective payment method for financial institutions and merchants. Checks comprise a decreasing percentage of the total noncash payment volume in the United States.* [2]*"*

Many institutions see electronic retail payment products such as remote deposit capture and remote ACH origination as the answer to many of the problems of traditional check fraud, but as the FFIEC observed in their recently updated IT Examination Handbook on Retail Payments:

> *"Electronic payment systems offer efficiency gains by allowing for rapid and convenient transmission of payment information among system participants. However, the emergence of a new payment mechanism can also enable the rapid propagation of fraud, money laundering, and operational disruption if data is compromised."*

The proliferation of remote electronic banking products, plus the increased sophistication of viruses and malware, have lead to an alarming increase in financial losses in the banking industry in recent years. For example Zeus, a virus that steals online banking details from infected computer users, is now more powerful than ever[3]. Recent lawsuits have been filed by customers against banks, and banks against customers[4], challenging the definition of "commercially reasonable" security measures, and perhaps now shifting the definition toward re-defining the ownership for the responsibility of security.

[1] http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.pdf
[2] http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.pdf
[3] http://news.bbc.co.uk/2/hi/technology/8634356.stm
[4] http://dockets.justia.com/docket/court-txedce/case_no-4:2009cv00653/case_id-120329/

A transaction is considered "high risk" if it permits the "movement of funds to other parties.[5]" The agencies of the FFIEC (Federal Reserve, FDIC, OTS, OCC and NCUA) consider transfer of deposit transaction information to represent the "movement of funds to other parties,[6]" and as such, necessitating stronger authentication and/or additional controls. Since remote (merchant-based) technology represents the highest level of the "high risk" category, we will further focus on the risks as they relate to remote deposit capture and remote ACH origination, and suggest some additional controls in these areas.

Risk and Risk Management

Effective management of vendor risk has always been important, and the new guidance places even more emphasis on this area. Examiners expect institutions to be able to identify and control risks associated with retail payment systems and related banking activities. In addition to the increased number of attack vectors and the increased velocity of the attacks, the management of retail payments risk is now even more difficult due to the increased reliance of the financial institution on third-party service providers. According to the FFIEC:

> *"Financial institutions increasingly rely on service providers, software vendors, and other third parties."*

and,

> *"Financial institutions are responsible for risks associated with the activities of third-party service providers with which they contract.[7]"*

The new guidance on Retail Payments makes it clear that institutions must establish and maintain effective vendor management programs, and must also understand how their service providers interact with other providers in the payment delivery chain. There are three opportunities for vendor oversight in the payment product lifecycle:

1. During the product selection process, <u>prior</u> to contracting for the product or service,
2. <u>After</u> the vendor has been selected, and <u>prior</u> to implementation, and
3. <u>Post</u> implementation, and <u>ongoing</u> as long as the vendor relationship exists

The requirements of your institution should determine the capabilities of the product. Once the capabilities have been defined, the Request for Proposal (RFP) should drive the vendor selection process. The RFP should describe the institution's objectives, the scope and nature of the work to be performed, as well as the financial institution's policies for security, business continuity, and change control. Once the institution receives responses to the RFP, it should evaluate the service provider capabilities against the institution's needs.

After the vendor has been selected, but before implementation of the product or service, the institution should complete the vendor due diligence process by evaluating broader issues such as

[5] FFIEC, Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment, August 15, 2006
[6] FFIEC, Risk Management of Remote Deposit Capture, January, 2009
[7] http://www.ffiec.gov/ffiecinfobase/booklets/tsp/tech_ser_provider.pdf

their experience and reputation, financial status, and resiliency of their systems.. Once the vendor is selected, and the product or service has been implemented, the vendor must be evaluated periodically (at least annually) to assure that the provider continues to deliver the quantity and quality of services required by the contract. The FFIEC Outsourcing Booklet has much more guidance in this area[8].

Vendors - Trust but Validate

Because the institution is heavily reliant on the vendor for the security of merchant-facing products and services, and because the institution is nonetheless responsible for the risks associated with these products, the institution must adopt a "trust but validate" approach, particularly with "high risk[9]" vendors when they supply and support high risk transaction products. Combining "trust but validate" with the principle of layered controls[10] means going beyond the standard checklist used by most institutions to periodically rank service providers by risk, and the standard checklist of controls (i.e. financial statements, SAS 70's, third-party reviews, etc.), to include additional control verification capabilities.

For example, many providers of remote deposit capture software have a built-in mechanism to detect if the transaction originates from other than a pre-approved IP address or range of addresses. The institution should also be able to detect, preferably through a separate mechanism, any change in the IP address and be able to respond accordingly. Additionally, since the vendor can only assure security of the transaction from the point of data entry into their software through transmission to their data center, there is still considerable risk assumed by the institution if a virus or other malware infects the host system. A key logger, plus the absence of true multi-factor authentication, can provide an attacker all the credentials necessary to initiate a funds transfer. The software vendor is not responsible for the security of the device on which it's installed, but the guidance makes it clear that the institution is responsible.

Identity Theft – Looking Beyond the Customer

Identity theft is also a growing concern among financial institutions (and regulators), and remote payment systems introduce a unique and potentially significantly expanded perspective on this, as responsibility for the confidentiality of customer information may extend beyond the institutions' customer. For example, consider the type of information entered into the remote deposit capture (RDC) merchant device. The merchants' customer presents a paper check, which is scanned into the device for transmission to the institution. Checks typically contain name, address, account number, ABA routing number, sometimes even phone numbers, drivers license numbers and even social security numbers. In short, more than enough information to pose a threat of identity theft, making the institution potentially responsible for risks to their customers' customer information if an attacker successfully penetrates an RDC device.

[8] http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf

[9] Although vendor management programs vary, vendors are generally classified as high risk if they either, 1.) Provide a critical service, or 2.) In the course of providing a non-critical service, have access to non-public customer information.

[10] http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf, page 17

Future Trends

Strong contracts may (and should) detail the security responsibilities on both sides, and the legal recourse if the terms of the contract are breached, but in most cases the institutions' recourse is limited to removal of the RDC device, and not the recovery of the financial loss. Regarding remote ACH and wire transfer, there are currently discussions in Washington about expanding Regulation E[11] to extend the same consumer protections in electronic funds transfers to commercial accounts. Whether this occurs, or new legislation is enacted, it's likely that it will favor the consumer, not the financial institution. But regardless of how responsibilities for fraud losses are determined, there is currently no transference of liability for financial losses from identity theft. This may be further tested and possibly redefined as current court cases are litigated later this year and early next. One potentially groundbreaking case is PlainsCapital Bank vs. Hillary Machinery. The customer originally sued the bank when the bank honored a series of wire transfer requests to overseas accounts after a cyber breach at the customer location was able to capture the ACH authentication credentials. Although the bank was able to recover most of the funds, the customer sued for recovery of the remaining loss. However, instead of reimbursing the customer, the bank made the unprecedented decision to counter-sue, alleging that the bank "at all times maintained commercially reasonable security measures within the meaning of 12 C.F.R. §§ 4A-201 and 4A-202.[12]" PlainsCapital Bank spokesperson John Floeter is further quoted as saying "…the cyber attack wasn't against our system[13]." This case promises to test the generally accepted view that the remote (merchant-based) devices are, by definition, functionally equivalent to a device located inside the banks internal network, and therefore subject to the same level of security.

Suggested Controls

Institutions are responsible for the privacy and confidentiality of customer data, regardless of where it may reside. The core vendors are currently working to address improvements in their security measures[14], but because community financial institutions are almost completely dependent upon the protection and security mechanisms provided to them by their vendor, and because the risks are real and immediate, they need to take the initiative to tighten security on their own.

So what can be done? The first step in controlling risk is to identify the assets to be protected, and the second step is to understand how risk manifests itself in your environment through a risk assessment. In order to grasp the potential impact of any non-specific threat to the enterprise, all relevant areas of risk must be considered. In their new guidance on Retail Payment Systems, the FFIEC states that:

> *"Management should develop risk management processes that capture not only operational risks, but also credit, liquidity, strategic, reputational, legal, and compliance risks"*

[11] http://www.federalreserve.gov/bankinforeg/reglisting.htm#E
[12] http://www.bankinfosecurity.com/external/Hillary-Complaint.pdf
[13] http://www.bankinfosecurity.com/articles.php?art_id=2349
[14] http://www.bankinfosecurity.com/articles.php?art_id=2451&rf=042410eb

We've already discussed the financial risk, and there is obvious and potentially substantial legal and reputation risk in a security breach as well. We've also discussed why addressing compliance risk by relying on vendor controls may not adequately address the risks in this category. Strategic risk is associated with the institution's overall mission, and how well a particular product or service contributes to the goals and objectives of that mission. Once again, vendor management is one of the keys to managing strategic risk:

> *"Because financial institutions are increasingly reliant upon third-party service providers for retail payment system products and services, the strategic plan should address comprehensive vendor management.*[15]*"*

As this paper was being written, the NIST had just issued their set of recommendations on protecting the confidentiality of personally identifiable information (PII)[16]. According to NIST, the two most important risk management controls are policy and procedure creation; and education, training, and awareness. I agree, and would propose a third control; a process that verifies that procedures are indeed being followed. This process would integrate documentation in the form of automated monitoring of key security metrics, combined with reporting and management oversight. Additionally, as NIST recommends, financial institutions should go the extra step and offer periodic training to their customers on information security best practices.

SUMMARY

Regulators consider "transfer of funds" technology as high-risk transactions. Allowing your customers to originate ACH and wire transfers from the convenience of their location is classified as a "transfer of funds", as such is subject to a much higher level of scrutiny. Compounding this problem further are recent court cases alleging that financial institutions failed to provide reasonable security for transactions originated at the merchant location.

Financial institutions must adequately assess and control the risks of remote electronic transactions in order to comply with the latest regulatory guidance, but they may need to go beyond the "compliance response". The controls suggested here may not eliminate the effects of financial, operational and reputation risk, but they may go just far enough to protect your organization.

SAFE SYSTEMS SOLUTIONS

Key security metrics should include, at a minimum, the presence and status of up-to-date antivirus, status of security patches, and the existence of a NAT enabled firewall. Our SafeCapture solution provides you with the following features:

- Easy installation of SafeCapture agent on all remote deposit capture workstations
- Monitor remote devices for patch levels and antivirus update levels
- Display date of latest virus definition file
- Display patch level
- Monitor if the PC is firewall enabled

[15] http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.pdf, Page 46
[16] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

- Monitor if the PC has a private range IP address
- Reporting included in our Quarterly Service Reports

SafeCapture provides your institution with a powerful risk management tool, assisting your institution in taking critical steps toward proper identification, assessment, and mitigation of remote deposit capture risk.

To find out how SafeCapture can help your institution mitigate remote deposit capture risk, contact Safe Systems at 877.752.0550 or info@safesystems.com.

About the Author

Tom Hinkel, Director of Compliance, is responsible for ensuring that Safe Systems' services incorporate and abide by appropriate financial industry regulations and best practices. In this position, Hinkel works closely with R&D, Product Management, and Operations Managers to ensure that new and existing services comply with FFIEC standards. Most importantly, by staying current on regulatory issues facing financial institutions, Hinkel serves as a regulatory compliance resource for Safe Systems' customers. With over fifteen years experience, initially on the engineering side installing and supporting bank networks and later in IT regulatory compliance, Hinkel's areas of expertise spans the entire spectrum of information technology. He has served on the inside as Manager of Information Systems, as well as Information Security Officer, and as an independent consultant for banks of all sizes from denovo to $1B+. Hinkel has been with Safe Systems, Inc. since 2005, most recently as an Account Manager. Hinkel holds a Bachelor of Arts degree from Illinois Wesleyan University, an Associate of Arts degree in computer programming, the GSEC security certification from the SANS Institute, and is currently studying towards the Certified Information Systems Auditor designation.

About Safe Systems, Inc.

Founded in 1993, Safe Systems is the national leader in providing compliance-centric IT solutions exclusively to financial institutions. As a technology partner, and recent winner of the MSP Best in Class Award by CompTIA and MSP Partners, Safe Systems has worked with over 500 financial institutions and manages over 16,000 network devices nationwide. Safe Systems' scalable and cost effective solutions include IT managed services, compliance solutions, business continuity and disaster recovery, network design and installation, security services, and IT and compliance training. Safe Systems helps financial institutions to significantly decrease costs, increase revenues, and improve performance. For additional information about Safe Systems, Inc., please visit www.safesystems.com or call 877.752.0550.