Fraud Versus Security

Too often security measures are confused with fraud prevention. Fraud, in the context of banking, pertains to the deliberate and specific theft of money or customer information through deception, misrepresentation and misuse of payment systems access. Security is the protection of information from compromise or attack and the authentication of individuals authorized to access the system for various purposes.

Regardless of the measures taken or the processes installed, there is not a substitute for KNOWING YOUR CUSTOMER. Offering high technology electronic payment products to customers that you hardly know, which enable them to tap into payments system at the speed of light ,without performing a comprehensive due diligence and credit review is not only dangerous but it is naive and a flagrant disregard of your responsibilities as a banking executive. Unlike a loan, giving access to a company or individual focused on fraud can impact hundred of thousands of individuals and involve millions of dollars in a very short period of time, regardless of the asset size of your institution. It is a global economy where technology can reach out to anyone, anywhere, anytime (24 x 7). Financial institutions must take a hard look at customers and potential customers that request access to high technology payment systems. A customer review should be more than a credit display on a loan application in front of the credit committee of your organization. Scrutiny must go beyond conventional review methods and look farther into the potential for fraud by the customer and their business history. A recent Ponzi scheme started in September 2005 and closed down in February 2006 by the SEC involved approximately 300,000 individuals and millions of dollars. It does not take much when you put the right tools in the wrong hands.

New Risk

Whether it is a substitute check or an original item, the risk of check fraud has always been there. Check 21 has not increased payment fraud risk; it has only made it more complicated. There are, however, detection and intervention measures that can be built into a system that will reduce some of the fraud risk to an organization.

Warning: System measures will not eliminate the risk entirely but can only reduce it. Your organization is responsible for managing the risk on a daily and, in some respects, per customer basis.

Risk Scenario

Prior to Check 21, check fraud could be perpetrated using paper checks, phone authorized drafts or ACH items, to mention a few. The phone authorized draft issue has been partially mitigated by the recently published final rule change to Regulation CC regarding the warranty of the deposited item. The final rule change shifts the warranty from the paying bank to the depositing bank. This is important because it closed an exploited weakness that existed in the payments system. Now more financial institutions will pay attention to deposited items and their customers. Before the rules change, the depositing institution did not have to pay attention to the deposited items and their customers when it came to Phone Authorized Drafts.

Under Check 21, the fraud mechanism is a simple one. The first scenario could involve an unscrupulous commercial customer having access, though your institution in the form of Remote Deposit Capture (Merchant) technology, ACH check conversion technology, also known as debit origination services, which is used to convert checks into ACH debits and then regular paper deposits. After scanning the check using the remote

deposit merchant capture product, the same check is scanned again using a separate system (one that is not integrated with the remote capture product), creating and transmitting an ACH file, then the original checks is deposited as an over-the-counter deposit at the teller window. One original check, but three separate deposits.

An alert account holder will see the three debits, notify their institution and have two of the three returned. However, these may go unnoticed for a period of time. If the debits represent recurring payments, they might not be noticed for several months. By that time, the depositing company may have folded up and disappeared.

Absent a fully integrated system that compares all transactions between Remote Capture, ACH and paper on the DDA system, there is only a limited defense. This can be through the posted deposit file extract and comparison of activity (after posting) from the three using product combined with a database program. It would be important that you create a history file that looks back as well as forward. The data attributes that you should look for are account number, routing and transit number, check number, and amount.

A variation of the above fraud would be the same commercial customer having a remote deposit remote merchant capture at one institution, ACH origination at separate institution and a conventional DDA relationship at a third institution. This would make the situation very difficult to monitor. There are techniques that are available that can reduce the risk.

An institution should not set up a customer and then walk away from the relationship and collect the fee income. This form of “Fire and Forget” sales is very dangerous. An institution needs to follow up after the sale with a comprehensive monitoring program that reviews the activities and transaction characteristics of the

customer. In this case and from your point of view, **Compliance is not optional!** It is a requirement!

Fraud Features

When selecting a remote capture system either in-house or outsourced you should look for systems that have all or some of these features:

- Front franking that is set by the financial institution. (After the item is originally scanned, the client passes the same check through the scanner a second time. The check will then be franked with a message that says "The item has already been scanned." This helps the customer from accidentally scanning the item twice. The item is not franked on the first pass in case the item is not read correctly and needs to be deposited manually.)
- Input edit limits (input only dollar amount and not manipulate the MICR line).
- Mod Checking of the Routing and Transit number
- File Limits (daily, weekly and monthly) with review and release options
- Duplicate file and duplicate item recognition and intercept
- File History duplicate review (minimum 12 months preferred 2 years)
- Volume monitoring with variance analysis (dollar value and transaction volume)
- Return Item monitoring
- Check Verification (Some systems today deploy a verification step. This verification can be to compare the scanned item against all of the checks processed by all of the customers being processed by the ASP. Others go out to a negative or positive file and attempt to match the item. This adds an additional step and aids in the validation of the item.)

These monitoring features, when combined with knowing your customer, will reduce your institution's risk of fraud.

Blended Solution

No one feature or interlock is going to be effective in mitigating all of the risk. A blended approach in features, periodic customer review and constant monitoring, however, will improve the likelihood that your organization will be able to manage the risk appropriately. An additional monitoring step would be to strip off a transaction file of the Remote Deposited items, the ACH items and the paper deposit and compare them against an historical database. This will aid in identifying duplicate items that have been deposited.

Information Theory (Push versus Pull)

Technology has changed the way we do business. Organizations, however, have not changed materially how business is monitored, reported on or managed. Understanding that is a stop gap, businesses need to transform how information is compiled and distributed. The most common approach today is to collect information in the form of extracts, files and reports. The data is compiled, printed out, and distributed in the form of a daily, weekly, monthly, or quarterly report. Most of the reports focus on revenue and all of them are after the fact! Reviewing a report a month after the fact does not bode well for managing risk and intervening when fraud is expected. This scenario is described as the "Pull" model when it comes to information management. The information needed, has to be pulled and compiled before it can be useful. Before you see the information, a significant amount of time has lapsed. To put this in perspective, when your customer can transact business, through your organization, 24 hours a day and

at the speed of light, looking at a customer report even a week later can be construed as being light years away from the original event! A timely response in regards to a fraud situation would next to impossible.

This information model needs to change. Organizations need to devise methods of monitoring customer activity that move away from the manual pulling and compiling of information. If it happens now, you need to know about it now. This approach is known as the "Push" model. Information on events and activities is pushed out to the parties that need it as it is happening, not after. Changes such as files sizes, return item volumes, transaction volumes, number of files per day or per processing period are events that should trigger a notification system that immediately involves management and senior executives. These systems can be used to notify the appropriate parties via an email message to a cell phone or PDA. The benefit of the Push model is that you can be informed of a situation immediately and thus be in a position to take action. The same theory can be applied to intervention activities that place the activity into a pending queue until reviewed and released. The Push model places the organization in control of the situation as it is occurring, as opposed to reacting months after the fact, while at the same time trying to figure out what happened.

Customer contract language should also be modified to include a clause that allows the financial institution to take immediate action in the event that fraud is suspected or suspicious activity is noticed. Today, the contract language requires customer notification in writing, preferably a certified letter with a return receipt and 30 days notice. That method may have been compatible with a paper based batch system but it is not compatible with a global, 24 by 7, electronic system. Financial institutions need

to be empowered to take immediate action. The contract language between you and your customer should clearly give you that power and authority. Your electronic enterprise needs to be protected.

The Ultimate Solution and Fraud Buster

Looking over the horizon, straight through processing systems (STP) are the future. Translating this into Remote Deposit, ACH and paper check deposit activity, these three products would be integrated on one system. Remote Deposit, Branch Capture (front or back counter) and ACH activity products all processed on the same platform and fully integrated with conventional DDA systems. Secondly, given that we are in an electronic world, each one of these transactions would be subjected to the same verification steps as an On-Line ATM or POS transaction. Before they are released, all transactions would receive a Pre-Auth, if not a negative or positive file verification (Telecheck, PPS and the like). I could even envision CVV-like keys issued for transaction accounts (DDA) at the transaction level that, if not properly authenticated, would cause the transaction to be rejected. The essence of future product development is not the elimination of paper checks as a choice, but the processing of paper items as though they were electronic.

Security

The financial institution has the primary responsibility of protecting the information and the systems that the information resides on from compromise and attack. Keeping a customer's information safe is just as important as keeping the customer's money safe. Take in mind that once the money is stolen, it is gone. If a customer's information is stolen, the impact of that theft can be felt by the customer and the

institution for years. That information can be misused and sold over and over again. It is the theft that keeps on stealing. Safeguarding the system, the information and the database must be priority one!

Each institution should have a security orientation section and training session with each customer that installs the Remote Deposit Capture (Merchant) product and the first item of business should be the discussion of what to do with the original checks after they are scanned.

- Do not throw them out with the trash.
- Do not keep the originals in a file folder or the customer payment record for an indefinite period of time (like forever).
- Do not make copies of all of the checks and shred the originals.

The customer should be instructed that after the original check has been successfully scanned and processed, the original item should be destroyed using, at a minimum, a "cross-cut" shredder. This should be done the next business day and after the client has verified the merchant capture file but held for no more than 24 hours, allowing for weekends. While the customer is waiting to verify the capture file, the original items should be locked up in a safe just like you would lock up cash. Why? With an electronic payments system, checks are like cash. They should be treated as though they are negotiable instruments.

Your financial institution needs to implement security measures, as well. Strong system security starts with the application developer understanding the concept of security and then building a security centric system. Ultimately, the best system is one that has an appropriate compartmentalization. From small business to large business,

having one individual with the system authority to do everything to anything is risky from two perspectives.

Strong system security

Having only one user within an application creates the equivalent of a super user (sometimes called administrator account).

Note: Having only one account will likely create several security issues. First, this account will likely have no restrictions on the types of configuration, or mis-configuration of the application.

Second, if everyone shares one account, you will no longer have accountability to the configuration or transactions which were conducted through the system. You lose the ability to see who did what and when they did it. Third, you won't be able to keep people's noses in their own responsibilities to get the job done. A super user account will have the ability to look around all of the application .

The vendor should be able provide templates for user *roles* within the system that will help clarify the typical security for the application and who's going to be using it on a daily, weekly, or monthly basis. For example, you may have a user in the application that only runs reports to deliver monthly. With individual users / passwords these things are possible. If there's only one user, chaos can ensue.

This super user account should be able to create new accounts to be used for regular, daily operations within the merchant. Theoretically, this account should also be

able to create and force password standards for the rest of the accounts. While your financial institution may have password standards, such as a minimum 5 character password with upper and lower case letters as well as numbers, the merchant should be able to set and adhere to their own password standards. They should also consider setting a time expiration on the password to ensure that the password changes from time to time. Even setting it at 6 months would be better than never. System Administrators are established at the financial institution level and at the customer level and each having a different type of security template depending on the system.

The selection of a super user system administrator at the customer location should not be taken lightly either. The risk is if a super user at the customer has their password and pin compromised, then the customer is exposed and in a majority of cases they won't even know it. In other words, you will be stark naked in a very cold wind! Not a very good position. The second perspective has to do with the defalcation side of the business. If a single user has the ability to run the system unchecked, unfortunate consequences can emerge. In either case the customer should be educated on the risks and responsibilities.

There are a number of applications that have good compartmentalization security features. Some of these features can be controlled and established at the institution level and managed by customer and some at the user level and managed by the customer. System level security pertains to the use of file encryption, a secure website "HTTPS:" and SSL (Secure Socket Layer) security between the host and should be considered as a minimum security set of features that an institution should look for before purchasing a

Remote Deposit product. Digital certificates are also a big plus, but are not as common as the previously mentioned security features. The vendor in either case should be able to help in establishing the right security levels for the right functions. One size does not fit all.

Features and functions that you should look for in providing compartmentalized security are:

- Bank level (established at system level by the financial institution):
- Front franking or "void" ink jet sprayed on the check after the check has been scanned
- Limited MICR Line repair (amount only input)
- Review and release (if established file limits are exceeded)
- Dollar limit (check size or file size)
- ACH Origination limits
- Database History limits (14 days as a rule of thumb)
- No local storage of scanned images on client desk top computer.

At the customer level, you should look for these security features:

- System administrator not defined as user
- User authority established (who can scan, who can correct, who can release)
- User file dollar amount limits
- User item dollar amount limits
- Batch files limits (number of items)

In all, the customer level security can vary from company to company and by user. The most important ingredient here, however, is not to put all of your security or functionality on the shoulders of one individual. The operation of the system should form a distributed authority perspective. This is the safest way.

Points to Consider:

- There is no substitute for knowing your customer.
- System measures will not eliminate the risk entirely but can only reduce it. Your organization is responsible for managing the risk on a daily and per customer basis.
- Follow up after the sale with a comprehensive monitoring program that reviews the activities and transaction characteristics of the customer.
- You should create a history file that looks back as well as forward. The data attributes to look for are account number, routing and transit number, check number, and amount.
- Create an ongoing monitoring program of activity in the following areas:
    - Dollar amount
    - Transaction volume
    - Return item (unauthorized debits)
- A significant increase in any of these areas or in return item volume in excess of the national average over a short period of time should be cause for alarm and trigger intervening action.
- When selecting a remote capture system either in-house or outsourced you should look for systems that have all or some of these features:
    - Front franking
    - Input edit limits
    - Mod Checking of the Routing and Transit number
    - File Limits (daily, weekly and monthly) with review and release options
    - Duplicate file and duplicate item recognition and intercept
    - File History duplicate review
    - Dollar and Transaction volume monitoring with variance analysis
    - Return Item monitoring

- Check Verification

- Remember, no one feature is going to be effective in mitigating all of the risk. A blended approach in features, periodic customer review and constant monitoring will improve your ability to manage the risk appropriately.

- Most organizations use the “Pull” model of information management, needed information has to be pulled from various filed and compiled before it can be useful. It is historical information.

- In the “Push” model, activity and event information is pushed out to the appropriate parties as it is happening via an email message to a cell phone or PDA.

