

Secure Check Printing in a Digital Age

- **Insights & Recommendations for Implementing
a Secure Check Disbursement Strategy**

Check Writing in a Digital Age – A White Paper

The Problem

For the purposes of this discussion and white paper, we differentiate between “check writing” and “check printing”. Check writing is the process of creating payment instruments to specified payees, for specific amounts and are considered to be completely negotiable. Most companies engage in check writing when paying employees or vendors. Check printing, on the other hand, is usually done by service bureaus and check printers like Deluxe, and produces blank checks in many formats to be filled out either manually or by computer and printer.

Check fraud is a global problem. In the United States alone, the U.S. Comptroller of the Currency stated that in 1996, check fraud losses in all industries totaled \$12 billion. According to the FBI’s 1994 Financial Institutions Fraud and Failure Report, 60 percent of all criminal referrals for indictment and trial can be traced to check fraud. Statistics from the banking industry and the FBI show that each year thieves steal more than 10 times as much through check fraud as they do through bank robberies.

The recent growth of check fraud can be attributed, in part, to advances in technology. Graphics software that retails for less than \$100 can create reproductions of almost any document, including checks. With a simple scanning device that costs under \$100 and a current annual report with a signed chairman’s letter, a thief can duplicate a CEO’s signature. Or, if an actual check is available, the treasury manager’s signature on the check can be run through the scanner. It costs only pennies to print blank checks filled in for any amount the thief chooses, signed by the appropriate corporate paying officer.

Finally, changes to the US Uniform Commercial Code resulted in the liability for cases of check fraud being more easily apportioned between banks and their corporate customers relative to a determination of fault. These changes make it even more important that banks and their customers exercise due diligence or “ordinary care” to prevent or minimize check fraud. Cooperative measures between banks and their customers, such as positive pay, create timely, closed loop detection of fraud occurrences.

Check fraud incorporates forgery, alteration, counterfeiting, paper hanging and check kiting. Each of the above requires specific measures in order to minimize their occurrence in any organization issuing checks on a regular basis.

The advent of MICR laser printers has offered both the potential of increased check fraud and at the same time has provided a new ability to control the process of producing checks in a more secure manner. This control, when properly implemented, can actually mitigate an organization’s risk. However, if an organization is to realize the benefits from this increased control, the process must be well understood and firmly secured by a multi-level security strategy.

When developing a secure document strategy, a common question is “How much is this going to cost us?” Before that question can be adequately answered another question should be asked first. “What is our overall exposure?” Only then will the first question have any relevance.

Who commits check fraud? Organized criminal groups with elaborate schemes to pass bad checks commit fraud. Individual criminals with sophisticated equipment alter or forge checks on a daily basis. Employees, vendor employees; in fact, anyone with intent and access to a scanner, a PC, a laser printer and check stock can commit fraud. In short, check fraud is virtually impossible to eradicate completely. An organization can, however, seek to drastically reduce its risk by incorporating a comprehensive, multi-level security strategy.

A Multi-Level Approach to Security to Deter Check Fraud:

- Physical Security**
- Electronic Security**

- ❑ **Organizational Security**
- ❑ **Process Security**

Physical Security

Restrictions on physical access to sensitive data and resources are an important step in the overall strategy. The first item to be controlled is, of course, your check stock. The paper and the printer should be kept in a secured location, with access limited to certain authorized personnel. This one measure, along with regular, but random, audits, is one of the most foolproof methods of preventing fraud. However, many organizations' business process requires that the printers and paper be accessible to a number of personnel. In this case, additional security, control, and accounting methods are necessary.

Building special features into blank safety stock and encoding certain information in a tamper resistant format also provide physical security. These features offer an additional and important building block in the foundation of secure check writing. Void pantographs, watermarks, colors, micro-printing, chemically sensitive paper (changes color when solvents are used), easy tear papers (to prevent tape liftoff), visible fibers, fluorescent inks, heat sensitive inks, and printed warnings on the check are all effective means, but by no means foolproof, of making check fraud more difficult. The security features above are readily available from manufacturers of safety papers. We strongly recommend that at least three of these types of features be incorporated in any blank check stock. An organization should advise its bank of the security features present in its checks as part of its due diligence, and it should do so in writing. Furthermore, the check stock itself should contain text that alerts the recipient (teller, etc.) to the security features present.

Serialized numbering of blank check stock can also be used to make auditing of stock usage easier and more controllable. Pre-printed stock serial numbers and software assigned check numbers do not have to agree (i.e., same number for both). The stock serial numbers simply provide a way to issue a fixed range of stock and to account for usage and waste.

The check printer can be physically secured through the use of a keylock, which prevents printing when in the OFF position or through the use of a password, either entered on the front panel or sent down from the host application. There are variations on this theme, with some printers providing a keylock that enables MICR printing, or standard printing, or no printing. The problem with these printers is that it is assumed that the MICR resources (MICR font and signatures) are resident in the printer and therefore access to them for printing can be controlled. Anyone with enough know-how can download a MICR font and a signature and print checks, even when the keylock is not in the MICR position. As a matter of fact, anyone can print a check, even without MICR toner, that will have a reasonable probability of being accepted and cashed by a bank teller. If "normal care" has been taken and documented by the issuer, the bank will most likely be liable in a case like this.

A printer can also have locking paper trays that prevent blank check stock from being removed while the printer is unattended. Some printers have locking output trays or locking covers to prevent removal of "written" checks by unauthorized personnel.

Electronic Security

Electronic security measures incorporate an array of preventative measures at various stages in the process. The first, and most important, is authentication via password of any and all users of software packages or systems that generate or contain check data or check writing resources (such as MICR fonts, signatures, etc.). This includes financial packages, check writing utilities, libraries, archives, and databases. It is further recommended that certain functions or events require a second and higher level password. Applications such as check reprint or occurrences such as "if amount exceeds" (signature level authority), should require a manager or supervisor to issue a second password.

System level (operating system) permissions that only allow authorized users or groups access to data files, resource libraries (folders), devices (printers), software programs, etc., are very effective in keeping unauthorized personnel from accessing critical resources and devices. Some platforms, notably IBM's AS/400 or iSeries, are given a high security rating by the US government when properly configured. Check writing security is greatly enhanced with these systems due to their inherent security and the "closely-coupled" relationship of output devices (printers) using IBM's AFP/IPDS proprietary print architecture and host operating system.

Device level print parameters that should be implemented in open systems (e.g., Windows NT/2000) are: disabling jam recovery, locking copy count modification at the printer, and locking of the front panel during check printing runs.

Encryption of datastreams when printing checks remotely is an additional but, in our opinion, not truly effective, method of preventing fraud. Since the only data being sent to the remote printer is the payee, check number, and amount field, it amounts to no more than an audit file. However, if MICR line information, the MICR font, signatures or any other proprietary information were also being sent simultaneously (with each check record), encryption would be an important security measure. In general, system security should be robust enough to protect the confidentiality of sensitive information transported over the organization's network. This should be part of an enterprise initiative for securing valuable data such as trade secrets, financial information, etc. Readily available protocols, including IPSEC for TCP/IP, work very well for point-to-point transmissions and can be utilized to provide authentication, encryption, and eliminate repudiation.

Organizations should consider an alternative method of generating manual checks, often done on a typewriter and using pre-printed check stock. Using a software package that has a "manual check" feature, prints to blank stock, that requires a password and generates an audit trail of manual or one-off checks issued is a good method.

An additional method, which has gained some interest in certain areas, is the inclusion of a barcode on the face of the check. The barcode may be as simple as 3 of 9 or as complex as PDF417 (2-D). The barcode could include the payee, check number, amount, and an encoded checksum digit, for example. Some check writing software packages provide the capability to incorporate these security features. While someone may alter the check, it would be far more difficult to alter the barcode. Of course, this presupposes that there is a closed process loop, i.e., that the receiving bank and bank of first deposit have the ability to read the barcode at the right time, i.e., at the teller's window. This requires an additional investment in a scanner and software, which most banks are reluctant to do.

Positive pay is a method by which the check originator creates an electronic file that lists the checks that were created, the amount, the date issued and the payee and forwards that information to their bank. The bank then compares checks that are processed (deposited) against this list and provides exception notices to the customer. Delineation of duties plays an important security role here also. The person who issues the checks should not be the same person who makes pay/no-pay positive pay exception decisions.

Reverse positive pay, a variant of the above, involves the transmission of MICR line information from the bank to the issuer on a daily basis, so that the issuer can compare presentment data with the issue data in their system. Usually, there is a time requirement for reporting an unauthorized or modified check back to the bank. This is an especially effective method for organizations that generate a large number of manual or on-demand checks, like insurance companies.

Time-sensitive notices on checks, such as "Not Valid After 90 Days" are a good way of putting yet another obstacle in the way of check alteration.

Image positive pay is a relatively new variant, with the bank providing digitized images of paid checks on a daily basis to the issuing organization.

Teller positive pay is an even more specialized service offered by some banks. With this service, tellers can detect fraudulent checks presented at the teller window of the bank on which the check is drawn because the teller systems are linked to customer issue files.

Finally, an audit report generated by the check writing utility, or in some cases the MICR printer, can close the internal security loop on the check writing process. Comparing the number of checks sent to the printer by the host software with a report of the actual output can help verify that no checks are missing and no duplicates have been printed. An exception report can be run electronically that will compare and kick out discrepancies between the two. Some larger MICR printers can capture check information digitally, using CCD arrays, as each check exits the printer into the output tray and create an uploadable file that can be compared against the issuing application's issued check list.

Organizational Security

Of all the security levels mentioned, an organization's internal security is the most vulnerable. Even the most comprehensive security strategy is rendered worthless when a password is divulged, a privileged workstation is left unattended, or check stock is left sitting out.

The saying "security begins at home" could certainly be applied to check writing. All organizations need to control availability and access to business-critical functions, devices and resources. A comprehensive and robust internal system security plan is the first and perhaps the most important step in securing the check writing process. All authorized users should be trained on the security procedures and periodically reminded of the importance of keeping all check writing resources secure.

The organization should consider delineating clear separation of duties: the person issuing checks should be different from the person charged with reconciling the accounts. A common source of check fraud comes from inside an organization. Someone creates a fictitious vendor and posts a payable to that vendor. The check to the fictitious vendor is printed during a regular check run and mailed, lost in the large number of valid checks issued and mailed.

Staff should be thoroughly trained in disbursing funds. The training should include a comprehensive review of legal and regulatory guidelines for disbursing funds, as well as the various types of common check fraud schemes used to steal money.

Process Security

Every conscientious organization should review its procedures regarding check writing and make appropriate changes if necessary. Are there adequate checkpoints and safeguards in place from the beginning of the process to the end of the process? Are the processes, such as check issuing and check reconciliation kept separate?

For example, how quickly do you reconcile your bank statement? Do you access your bank account(s) online once a week or better yet, daily, to review the checks that have cleared your bank against those you have written? Do you use an audit trail report after each check run to verify that all checks are accounted for? Do you control and account for all check stock, even that which is destroyed? Has your systems team verified that all sensitive electronic resources and devices are secured by password control and access authority? Do you change passwords on a regular basis?

Summary

Check fraud has always been rampant. However, with advances in, and ready availability to, sophisticated technology, it has become a lot easier. As with most security schemes, any strategy can be circumvented eventually. What is important is a multi-level approach, incorporating features addressing each of the above mentioned areas. Periodic and random reviews and audits are an excellent way of determining the effectiveness or appropriateness of a given strategy and

are highly recommended. While check fraud may never be eliminated, it can be greatly minimized with planning and execution of a sound security strategy.

Since checks will be the most common method of making payments for many years to come, you need to safeguard your organization against check fraud.

- ❑ Use a positive pay service on all disbursement accounts.
- ❑ Reconcile accounts promptly – daily if possible.
- ❑ Consider online reporting and reconciliation services.
- ❑ Consider a highly secure check writing solution and platform that provides additional security features.
- ❑ Use check stock with fraud prevention security features.
- ❑ Keep check stock under lock and key.
- ❑ Restrict access to check writing programs, MICR printers and check resources (signatures, MICR font, etc.)
- ❑ Make frequent, unannounced audits of your check stock.
- ❑ Limit the number of signatures, and immediately notify your bank of changes in signing authorization.
- ❑ Separate the check writing and account reconciliation functions.
- ❑ Separate the purchasing and check writing functions.
- ❑ When possible, use maximum payment limits on accounts.
- ❑ Set up a separate account for large dollar payments.
- ❑ Use an information reporting service providing daily reports of checks above a minimum dollar threshold.

The Company

Rosetta Technologies Corporation has been engaged in developing check-writing/printing systems since the 1980s. As a full-service vendor and manufacturer, the company develops MICR laser printers for workgroup and production environments, software packages for check printing and payments, and offers a complete line of precision manufactured MICR consumables and safety check stock. The company is a standing member of the ANSI X9b Accredited Standards Committee for Paper Payment Systems.

Author: Robert W. Hullar

Contributors: Peter J. Kusterer, Andrew Pease, Paul Malinowski

Sources: Bank of America, Federal Bureau of Investigation, US Comptroller of the Currency

To learn more:

www.rosettatechnologies.com

Or contact us at:

Toll-free: (800) 937-4224

(813) 623-6205

Fax: (813) 620-1107

Or email us: info@rosettatechnologies.com