

# Bank Fraud & IT Security

Prepared by  
Southeast Consulting, Inc.

SCI

June 2008  
Volume 6, Number 6

## REPORT

### Check Fraud Liability

by Frank W. Abagnale, Document Security Consultant

Holder in Due Course (HIDC) is part of the Uniform Commercial Code (UCC) that significantly impacts an organization's liability for check fraud from the checks it issues. After learning about HIDC, prudent companies are often motivated to use high security checks and change check disbursement procedures to protect themselves. Anyone responsible for check disbursements or fraud prevention should understand this law. Accordingly, the following is a brief description of Holder in Due Course along with four instructive federal appellate court rulings.

In simple terms, a Holder in Due Course is anyone who accepts a check for payment. On the face of the check, there neither evidence of forgery or alteration, nor does the recipient have knowledge of any fraud related to the check. Under these conditions, the recipient is an HIDC and is entitled to be paid for the check.

The statute of limitations under the UCC for an HIDC to sue the check's maker for its face value is 10 years from the issue date, or three years from the date the check was first deposited and returned unpaid, whichever comes first. An HIDC can assign, sell, give, or otherwise transfer its rights to another party, who assumes the same legal rights as the original holder.

The following four federal appellate court cases illustrate the far-reaching power of *Holder in Due Course*.

- **Robert J. Triffin v. Cigna Insurance**  
*Issue: Placing a stop payment does not eliminate your obligation to pay a check.* In July 1993, Cigna Insurance issued James Mills a workers' compensation check for \$484. Mills falsely claimed he did not receive it due to an address change and requested a replacement. Cigna placed a stop payment on the initial check

### Table of Contents

- Check Fraud Liability.....1
- The Role of the Independent Auditor in Detecting Bank Fraud.....4
- How Much of Your Bank's Data Is in the Wild?.....6

### Editorial Board

**Frank W. Abagnale**, *Abagnale & Associates*  
**Rich Baich**, *Principal, Deloitte & Touche LLP*  
**Tom Bartolomeo**, *Senior Vice President, Information Security, Wachovia Corporation*  
**James Bauerle**, *Esq., Legal and Fraud Prevention Services, Keevican, Weiss, Bauerle and Hirsch*  
**Dr. Bill Chu**, *Chairman, Department of Software and Information Systems, University of North Carolina at Charlotte*  
**Robert Dinsmore**, *Audit Committee Chairman, American Community Bancshares*  
**Steve Hasty**, *Partner-in-Charge, Regional Risk Advisory Services, KPMG, LLP*  
**Jim Mathews**, *SVP/Bank Security Officer, First Charter Bank*  
**Robert Siciliano**, *IDTheftSecurity.com*  
**Ralph Summerford**, *President, Forensic/Strategic Solutions, PC*

### A.S. Pratt & Sons

2008 © ALEX eSOLUTIONS. All rights reserved.  
The ALEX eSOLUTIONS logo is a trademark, used herein under license.

### Need more information on specific topics?

**Call:** 800-572-2797  
**E-mail:** [info.pratt@aspratt.com](mailto:info.pratt@aspratt.com)  
**Visit:** [www.aspratt.com](http://www.aspratt.com)

and issued a new check. Mills nevertheless cashed the first check at Sun's Market (Sun). Sun then presented the check for payment through its bank. Cigna's bank dishonored the check, stamped it "Stop Payment," and returned the check to Sun's bank.

Had Sun filed an HIDC claim against Cigna as the issuer of the check, Sun would have been entitled to be paid because of its status as a Holder in Due Course. Apparently, Sun either did not know about HIDC or chose not to pursue it. Sun management merely pinned the check on a bulletin board in the store, for two years.

Eventually, Robert Triffin bought the check from Sun, assumed its HIDC rights, and filed a lawsuit in August 1995, over two years after the check was returned unpaid. Remember that the statute of limitations is three years. The court ruled in favor of Robert Triffin and ordered Cigna to pay him \$484 plus interest.

*Recommendation:* Cause a check to *expire* before replacing it or you may be held liable for both checks. This can be facilitated by printing an expiration statement on the check face such as, "THIS CHECK EXPIRES AND IS VOID 20 DAYS FROM ISSUE DATE." If a check is lost, wait 20 plus 2 days from the initial issue date before re-issuing. Many companies print "VOID AFTER 90 DAYS" but cannot reasonably wait that long before re-issuing a check. A party that accepts an expired check has no legal basis to sue as an HIDC if the check is returned unpaid.

Superior Court of New Jersey, Appellate Division, A-163-00T5. <http://lwlibrary.rutgers.edu/courts/appellate/a0163-00.opn.html>

**After learning about HIDC, prudent companies are often motivated to use high security checks and change check disbursement procedures to protect themselves.**

- ***Robert. J. Triffin v. Somerset Valley Bank and Hauser Contracting Co.***

*Issue:* You may be held responsible for checks you did not issue or authorize. Hauser Contracting Co. used ADP for payroll services. A thief obtained check stock that looked identical to ADP's checks and created 80 counterfeit payroll checks totaling nearly \$25,000. These coun-

terfeit checks were identical to Hauser Contracting Co.'s.

A retailer who knew Mr. Hauser became suspicious and called him. Somerset Valley Bank also called. Mr. Hauser reviewed the in-clearing checks, which looked just like his, and confirmed the checks were unauthorized and the payees were not his employees. The bank returned the checks marked as "Stolen Check — Do Not Present Again."

Mr. Triffin bought 18 of these checks totaling \$8,800 from four check-cashing agencies, claimed HIDC status, and sued both Mr. Hauser and his bank for negligence for not safeguarding the payroll checks and facsimile stamp. Because the counterfeit and authentic checks looked identical, the lower court ruled for Triffin.

Hauser appealed, but the federal appellate court upheld the lower court. The court said the counterfeit check met the definition of a negotiable instrument and, because the check and signature were identical to an authentic check, the check-cashing agency could not have known it was not authentic.

*Recommendation:* Use a controlled check stock, which means using checks that are uniquely designed or customized for your organization and are not available blank to others. SAFEChecks and the SuperBusiness-Check are controlled check stocks.

Superior Court of New Jersey, Appellate Division, A-163-00T5. <http://lawlibrary.rutgers.edu/courts/appellate/a0163-00.opn.html>

- ***Robert J. Triffin v. Pomerantz Staffing Services, LLC***

*Issue:* High security checks may protect you from some holder in due course claims. Pomerantz Staffing Services used high security checks that included heat sensitive thermo chromatic ink on the back and a warning banner on the face that said, "THE BACK OF THIS CHECK HAS HEAT SENSITIVE INK TO CONFIRM AUTHENTICITY." Someone made copies of Pomerantz's checks, but without the thermo ink on the back. They cashed 18 checks totaling \$7,000 at Friendly Check Cashing Company. Friendly's cashiers failed to heed the warning on the check face and did not look for the thermo ink. All 18 checks were returned unpaid, likely caught by Positive Pay.

Mr. Triffin bought the checks, claimed Holder in Due Course status, and sued Pomerantz. Pomerantz countersued and won. The judge correctly asserted that if Friendly had looked for the thermo ink as instructed, they could have determined that the checks were counterfeit. Because they were provided a means to verify authenticity and failed to do so, they were not an HIDC and had no

rights to transfer to Mr. Triffin.

This case illustrates the value of check security features, a properly worded warning band, and a controlled check stock. Pomerantz was protected by his checks.

*Recommendation:* Use high security checks with overt and covert security features, including explicitly worded warning bands. Such security features will also help prevent other kinds of check fraud. The SuperBusinessCheck is a properly designed high security check with 16 security features.

<http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html>

- ***Arkwright Mutual Insurance v. NationsBank***

*Issue: Facsimile signatures may invite fraud losses.* In another victory for banks, the Florida 11th Circuit Court of Appeals upheld NationsBank's, now Bank of America, interpretation of its carefully worded Deposit Agreement. This agreement effectively shifted the burden of responsibility from the bank to its customer in cases of forgery. The phrase "purporting to bear the facsimile signature" saved NationsBank over \$4 million in losses resulting from forged checks.

***Banks are bound by the regulations of the UCC, which has historically placed the responsibility for detecting forgery on the bank. However, the UCC also specifically allows a bank and its customers to alter, through contractual agreement, the liability for fraud losses.***

Florida Power and Light (FP&L), a customer of NationsBank, used a facsimile machine to sign most of its corporate checks. FP&L's check volume totaled nearly 20,000 each month. Unfortunately, in the mid-1990s, 27 fake checks were cashed over a two-month period totaling \$4,387,057. These counterfeit checks bore exact replicas of the FP&L facsimile signature and used actual serial numbers from real FP&L checks that had been voided or cancelled.

Because all of the counterfeit checks were over the

\$25,000 sight review threshold established by NationsBank, each one was sent to the Signature Control Department and visually compared with the authorized signatures. The fake checks appeared authentic and signatures were identical to the signature cards, and therefore, were paid *in good faith*. When FP&L discovered the counterfeits, they contacted NationsBank, which in turn contacted its upstream collecting banks. However, because the 24-hour rescission period had long since passed, NationsBank was denied its request for reimbursement. It therefore refused to credit FP&L for the loss.

Arkwright Mutual Insurance, who insured FP&L against commercial crime, reimbursed the company. It then sued NationsBank. Arkwright claimed that the checks were not *properly payable* because nothing in the contracts between the two had authorized NationsBank to pay checks with forged facsimile signatures.

NationsBank disputed this, pointing out that FP&L had agreed to a provision in its Deposit Agreement that said, "If your items are signed using any facsimile signature or non-manual form of signature, you acknowledge that it is solely for your benefit and convenience. You accept sole responsibility for maintaining security over any device affixing the signature. Such signature will be effective as your signature regardless of whether the person affixing it was authorized to do so."

As part of the Deposit Agreement contract, FP&L had passed a resolution authorizing NationsBank to pay checks for \$500,000 or less *when bearing or purporting to bear* selected facsimile signatures.

This is extremely significant. Banks are bound by the regulations of the Uniform Commercial Code, which has historically placed the responsibility for detecting forgery on the bank. However, the UCC also specifically allows a bank and its customers to alter, through contractual agreement, the liability for fraud losses. The code states:

The effect of the provisions of this chapter (4-103) may be varied by agreement, but the parties cannot disclaim a bank's responsibility for its lack of good faith or failure to exercise ordinary care or limit the measure of damages for the lack of failure. However, the parties may determine by agreement the standards by which the bank's responsibility is to be measured, if those standards are not manifestly unreasonable.

In other words, the parties may set their own ground rules as long as it is not overly one-sided.

The official comments to Chapter 4-103 expand on this idea:

In view of the technical complexity in the field of bank collections, the enormous number of items

handled by banks, the certainty that there will be variations from the normal in each day's work in each bank, the certainty of changing conditions and the possibility of developing improved methods of collection to speed the process, it would be unwise to freeze the present methods of operation by mandatory rules. This section, therefore, permits within wide limits variation of the effects of provisions of this Article by agreement [Subsection [1]] confers blanket power to vary all provisions of this Article by agreements of the ordinary kind.

The Florida court granted summary judgment to NationsBank, agreeing that these two contractual agreements shifted the liability for the forged checks to Florida Power and Light.

Clearly, the courts are upholding the freedom-of-contract language between banks and their customers, requiring a company to abide by the agreements it has signed. These legal precedents should encourage banks to be precise when drafting documents outlining customer responsibilities with respect to fraud, and customers to read, fully understand, and agree *to the fine print*.

**Conclusion:** Implement fraud prevention measures, such as Positive Pay and highly secure controlled check stock, which would have caught the forged checks and in this case stymied the forger.

## The Role of the Independent Auditor in Detecting Bank Fraud

by Dr. Casper Wiggins, University of North Carolina – Charlotte

Major frauds within the last several years have received much media attention and have cost financial institutions, corporations, employees, shareholders, and the public billions of dollars. Many organizations have gone out of business or declared bankruptcy, employees have lost their jobs, and pension beneficiaries and shareholders have lost significant investment value. Additionally, the general public has incurred increased costs for goods and services, all due to an escalating volume of fraud.

The Sarbanes-Oxley Act was passed by Congress in 2002 to increase the public's confidence in financial information provided by financial institutions and public companies while deterring the occurrence of fraud. This act has significantly increased the costs to public companies and accounting firms as a result of procedures

required to comply with the act's provisions, regulations, and guidelines. Further, the act has strengthened penalties for corporate fraud, created the Public Company Accounting Oversight Board to oversee accounting firms auditing financial statements of public companies, while enhancing corporate governance.

**The Fraud Problem.** The seriousness of fraud has been widely publicized by losses incurred by employees, shareholders, accounting firms, and others. In addition to those companies where fraud has been reported in the media, the results of a number of surveys have been issued that indicate that fraud is a major global problem incurred by companies and financial institutions that have not had their fraud experience publicized. In fact, it has been estimated that only 20 percent of discovered frauds have been exposed through the media.

Two recent surveys indicate that fraud appears to be a particularly serious problem for financial institutions. For example, a global survey sponsored by a major international accounting firm indicated that 37 percent of the responding companies had suffered from serious frauds during the previous two years. Those respondents exposed to fraud indicated an average loss of over \$2.5 million.

The banking and financial services industry has been particularly hard hit by fraudsters. Financial services companies, including banking and insurance, reported more incidences of fraud than other industry segments in recent surveys. Another international survey reported that almost half of the survey respondents who suffered more than 50 frauds in a 12-month period were predominantly from the banking and financial services sectors. Three of these financial services sector frauds totaled more than \$25 million each. Additionally, the *Financial Institute Fraud and Failure Report* for the most recent reporting period issued by the FBI indicates that over 250,000 Suspicious Activity Reports (SARs) involving fraud were received from April 1 to September 3. This report further indicates that 47 percent of all SARs were filed by U.S. financial institutions. Moreover, the losses associated with these financial institutions-related SARs equaled approximately \$9 billion.

### Types of Fraud Crimes and Who Commits Them.

The two types of fraud that affect financial statements are *management fraud* and *employee embezzlement*. Management or financial statement fraud involves management's deceptive manipulation of financial statements with the objective of misleading investors and creditors as to the financial condition of the financial institution.

Employee embezzlement occurs when an employee directly or indirectly steals from his or her employer. In

many cases, the costs associated with these thefts are not reported in the company's financial statements because the loss has not, as of yet, been discovered.

Misappropriation of assets is the most widely reported type of fraud. PricewaterhouseCoopers' 2006 *Global Economic Crime Survey* indicated that 60 percent of all reporting victims cited incurring this type of fraud. Moreover, the *Ernst & Young International Fraud Survey* for 2007 indicated that a majority of survey respondents were more concerned about misappropriation of assets than any other type of fraud. However, less than 20 percent of these respondents were concerned about financial statement fraud. Only 10 percent of the respondents of the PricewaterhouseCoopers' survey indicated experiencing financial statement fraud.

The 2007 *Report to the Nation*, issued by the Association of Certified Fraud Examiners, indicates that approximately 86 percent of all fraud cases were concerned with misappropriation of assets while only 5 percent were concerned with fraudulent financial statements. However, the length of time to execute a misappropriation of assets scheme is shorter, requiring less than 18 months compared to that involving financial statements fraud, which typically extends for two years. These statistics indicate that misappropriation of assets schemes may be easier to detect.

Internal controls appear to be more effective in preventing or detecting asset misuse than in identifying fraudulent financial statements. Accordingly, it may be more difficult to detect financial statement fraud due to management's ability to override internal controls, systems, and procedures.

What is more, surveys show that fraud schemes committed by managers and executives are more costly to the organization than fraud committed by rank and file employees. This fact is further illustrated by the Association of Fraud Examiners' report that indicates a median loss of \$250,000 caused by managers and executives as compared to \$70,000 caused by other employees. Finally, the 2007 Ernst & Young Survey reported that company managers were responsible for 55 percent of the internal fraud as compared to 30 percent caused by other employees.

**Fraud Prevention Is the Key!** Prevention is the most effective means of eliminating losses from fraud. The best way to prevent fraud is to eliminate the opportunity for fraud while promoting a corporate culture of honesty and integrity. To eliminate opportunities for fraud, management must design and implement a control system that protects the company's assets from theft while ensuring the integrity of the financial statements. Controls that relate directly to the reliability of the financial statements

involve the control environment, the accounting information system, and the control processes.

The control environment involves factors that include the following elements:

- Integrity and ethical values
- Commitment to competence
- Strong board of directors and audit committee
- Positive management support philosophy
- Effective organizational structure
- Appropriate assignment of authority and responsibility
- Effective, well-documented, human resource policies and practices.

The accounting information system consists of methods and records established to record, process, summarize and report an entity's transactions while maintaining accountability for the related assets, liabilities, and equity. Control processes must include policies and procedures which pertain to performance reviews and information processing. Physical controls and segregation of duties are used to help ensure that management directives are properly carried out.

***The best way to prevent fraud is to eliminate the opportunity for fraud while promoting a corporate culture of honesty and integrity.***

Corporate management has the responsibility to model appropriate behavior and to communicate to company employees that unethical behavior will not be tolerated. A code of business ethics must be enforced to provide guidance as to what management considers unethical behavior. Unrealistic performance goals and executive compensation plans that tie management's compensation to reported income can frequently foster unethical and inappropriate executive behavior.

**Detecting Fraud.** Combating fraud requires the combined efforts of both management and independent auditors. Management has the responsibility to design and implement internal controls to protect company assets and to provide accurate financial statements to shareholders, creditors, and regulatory agencies.

The independent auditor is responsible for providing an opinion on the company's financial statements as to

whether or not the statements are free of material misstatements. Material misstatements are errors and omissions that are large enough to cause the financial statements to be misleading to investors and other users.

It is important to note that it is the auditor's duty to perform audit procedures designed to provide reasonable assurance of identifying and requiring adjustments for material misstatements, regardless of whether or not fraud is involved. In fulfilling this responsibility, the auditor must assess the risks of misstatement, exercise due care and professional skepticism in carrying out the audit and documenting the results of his or her findings. It is important to recognize that it is not the independent auditor's responsibility to detect all instances of fraud that might have occurred. Rather, the independent auditor is only responsible for detecting fraud that rises to the level of causing the financial statements to be misleading, and thus invalidating the audit opinion.

Statement on Auditing Standards (SAS No. 82), entitled *Consideration of Fraud in a Financial Statement Audit*, was issued in 1997 to provide independent auditors with guidance to obtain reasonable assurance that financial statements are free of material misstatements related to fraud. SAS No. 99, which was issued in 2002, revised SAS No. 82 and included expanded guidance and minimum procedures for detecting fraud. This revised statement also provides recommendations for company management to develop processes for enhancing fraud prevention and detection activities.

The independent auditor must also report on management's assessment of the effectiveness of internal control under the Sarbanes-Oxley Act. Management's requirement to assess the internal control structure as well as the auditor's attestation to this assessment should help prevent and detect fraud caused by inadequate controls in publicly held companies.

Because of the limitations of an audit and the difficulty of detecting fraud, the independent auditor cannot provide absolute assurance that financial statements are free from material misstatements due to fraud. Fraud may be concealed through collusion among management, employees, or third parties. Management as well as those having oversight responsibilities for the financial reporting process, such as the audit committee, board of trustees, board of directors, or owners in owner-managed entities, must create and maintain a culture of honesty and high ethical standards. Although management has the responsibility to establish controls to prevent, deter, and detect fraud, both the independent auditor and others who have oversight responsibilities must assure that management has established proper controls and that these controls have not been compromised.

Internal audit departments can provide valuable assis-

tance to both audit committees and independent auditors in monitoring controls and helping management design policies to prevent fraud.

**Red Flags and Hotlines.** Auditors as well as employees must be aware of the red flags of fraudulent activities. Steve Albrecht, a nationally recognized fraud examination expert and BYU accounting professor identifies the following red flags or symptoms of fraud:

- Unusual items or errors in accounting records or documents
- Weak internal controls
- Unusual relationships, actions, transactions amounts, events, or procedures
- Changes in the lifestyles of employees
- Unusual behavior, attitude changes, or emotional displays by employees

**Tips and Complaints.** Fraud is most commonly detected through tips. Therefore, an effective tip hotline system should be adopted which permits employees to anonymously report suspicious acts, preferably to security agents outside of the company. Because of the severity of bank fraud problems, financial institutions must take a comprehensive approach to preventing and detecting fraud. When fraud is discovered, perpetrators must be prosecuted criminally and civilly. Failure to do so will only send a message to other employees that your bank is not serious about fraud.

## How Much of Your Bank's Data Is in the Wild?

by T. Herbert Alban, Netec Security Advisors

Just how much sensitive corporate data resides on your bank's peer-to-peer networks waiting to be pilfered by cyber thieves? While it seems highly unlikely that such banking data could be so easily available on the Internet, a recent technical search of peer-to-peer (P2P) networks yielded reams of confidential business documents, including spreadsheets, billing data, health records, requests for proposals, internal audit reports, new product specifications, and confidential meeting notes. All of this proprietary data was easily found using simple search tools.

While we thought it doubtful that so many people were deliberately sharing such sensitive data, we speculated that many users or perhaps their family members had installed P2P programs to download music, movies,

or even newscasts. When installing such a P2P download program, it is easy to simply click OK to all of the questions during the install process. One of these install selections is typically which folder from which to share files. Many people select the default mode, which is the *Windows My Documents*, folder during this step in the setup process. The result of this simple selection can be devastating. This is because the default selection will make networked files readily available to the Internet, leaving no trace of when the files are uploaded or copied. Accordingly, it is clearly time for bank IT security managers to add P2P file sharing to their bank's list of security threats and concerns.

**Dangerous P2P Protocols.** There are several popular P2P protocols, each with a number of client programs that can access a network. While actual user numbers are difficult to come by, BitTorrent is thought to be the largest P2P network, with more than 10 million users of its most popular tracker sites. Tracker sites are designed to track the whereabouts of P2P files so they can be accessed. BitTorrent operates differently from other P2P networks in that a user must take deliberate steps to share a file. BitTorrent is also the network that is most popular for legitimate purposes. For this reason, much of our nation's open source software is distributed via BitTorrent.

***A recent technical search of P2P networks yielded reams of confidential business documents, including spreadsheets, billing data, health records, requests for proposals, internal audit reports, new product specifications, and confidential meeting notes.***

The Gnutella network, like several other P2P networks, lets you browse all of the files that a remote computer is sharing. This allows you to quickly shift from search results to related files from the same user.

Gnutella's most popular client, LimeWire, has a market share of more than 35 percent of all P2P clients and is estimated to be installed on approximately one-fifth of all computers. Other client software with a sizable installed base includes Kazaa, Morpheus, and Soulseek.

The LimeWire Pro version allows connections to more servers, which allows you to uncover more data

in a shorter time period. Choosing good search terms is essential when conducting P2P data searches. Since Gnutella supports only file-name searches, it is important to assemble a list of relevant search terms, such as "audit report," "request for proposal," or "meeting minutes." It is also important to limit searches to *documents* thereby avoiding being inundated with results for media files. A recent search for the term "audit report" turned up numerous results, none of which proved promising. Accordingly, the researcher deployed LimeWire's connections tab to remove all of the servers to which the researcher was connected. This caused LimeWire to reconnect to other servers.

Gnutella is unique in that it has no central server cataloging shared files. This allows every client to appear as a server. Accordingly, if a search with one set of servers does not turn up your desired results, then try different servers. This approach will provide varied views of the files on the network.

Once the researcher clicked on *Get More Results*, they quickly discovered a file with a promising name: *internal audit plan*. This is where the true power of LimeWire's *Browse Host* button is realized, as it allowed the researcher to explore all of the files shared by that computer. This search yielded a valuable lode of documents. Along with the internal audit plan, the researcher found audit results from several engagements, interview notes from internal investigations, and numerous corporate financial statements.

A second search focused on new search terms and plowed through dozens of computers full of mundane data until the researcher entered *ssn* for social security number. LimeWire, which displays the IP address of the computer hosting each file a search returns, showed an entire page of results for *ssn*, all with the same IP address. Using browse host, the researcher discovered a plethora of bank passwords and credit card numbers, numerous files labeled as credit bureau reports, and a handful of individual tax returns.

What the researcher had stumbled upon is known as an information concentrator. Concentrators are usually hosted by cyber theft rings who scan P2P networks for files with personal data. Their intentions are typically criminal, focusing primarily upon identity theft. Most likely these cyber thieves had inadvertently posted the confidential information they had found, making the same mistakes with P2P that their prey had made.

**Root Cause.** As the researcher honed his technique, he generated more reliable results. The search term "minutes" led the researcher to what looked like the computer of a high level staffer of a national political party. This discovery included files that identified the home and cell

phone numbers of senators, confidential meeting notes, and fund-raising plans.

Among all of this, a pattern emerged. Someone was sharing a large number of new product design specifications and product orders, each labeled with the major retailer that had ordered the designs, along with correspondence between the suppliers and the manufacturers concerning the orders.

**There are several popular P2P protocols, each with a number of client programs that can access a network.**

Another person appeared to be the owner of a cell-tower consulting firm. During this search, the researcher discovered files with site surveys and feasibility studies of various tower locations for several national telecommunications carriers. Had the researcher been inclined, he could have purchased various real estate locations for which no suitable alternative locations were mentioned, and then lobby the utility company for a high purchase price.

The researcher realized that most large companies have security measures to prevent data leaks. However, most small suppliers and business partners entrusted with confidential data do not. It was further realized that it was mostly these small businesses, probably without any IT support or formal security policies, that were leaking large quantities of corporate data.

Based on what the researcher discovered with these simple tools in a short time, it is clear that there is really a lode of important corporate data coursing through P2P networks. Accordingly, it is essential that your bank not just implement strong policies and preventive measures covering your bank's computers and networks, but also address those used by employees at home and the practices of partners and suppliers.

You can test your peer-to-peer network data exposure in the wild by following these basic research steps:

1. *Build a list of keywords from the names of important files.* Be specific, as unique industry jargon makes for ideal searches.

2. *Keep search phrases short, as LimeWire has a limit of 30 characters.* Search only for documents. In this way, you will not get inundated with media files.
3. *Go to Tools>Options>Sharing to be sure you are not sharing confidential materials.* Safer yet, run LimeWire in a virtual machine mode.
4. *Once you find a file that looks like it belongs to your financial institution, select it and choose Browse Host.* This will allow you to examine other files that are being shared. Note the IP address so you can track down the user sharing the files.
5. *After a search, select all listings under the Servers tab and click the Remove button.* This will drop those connections and add different servers. Then right-click on the search tab and choose *Select More>Get More Results* to extend your search. Repeat this several times to broaden your search as widely as possible.

## BANK FRAUD AND IT SECURITY REPORT

### Editor

Peter A. Mihaltian, President  
Southeast Consulting, Inc.  
212 S. Tryon Street, Suite 1680  
PO Box 470886  
Charlotte, NC 28247-0886  
(704) 338-9160  
E-mail: [SECI@aol.com](mailto:SECI@aol.com)  
Web site: [www.southeastconsulting.com](http://www.southeastconsulting.com)

### Publisher's Staff

Manuscript Editor  
Diane Calmes  
  
Editorial Inquiries  
Peter A. Mihaltian

BANK FRAUD AND IT SECURITY REPORT (ISSN 1546-4105) is published monthly by A.S. Pratt & Sons Group, 805 Fifteenth Street, N.W., Third Floor, Washington, D.C. 20005-2207. Copyright ©2008 by ALEX eSOLUTIONS, Inc. All rights reserved. No part of this newsletter may be reproduced in any form by microfilm, xerography, or otherwise incorporated into any information retrieval system without the written permission of the copyright owner. Requests to reproduce material contained in the publications should be addressed to Copyright Clearance Center, 222 Rosewood Drive, Danvers MA 01923, (978) 750-8400, fax (978) 750-4470. For customer service information, call (800) 572-2797. EDITORIAL INQUIRIES: Direct to SCI.

POSTMASTER: Send address changes to BANK FRAUD AND IT SECURITY REPORT, A.S. Pratt & Sons Group, 805 Fifteenth Street, N.W., Third Floor, Washington, D.C. 20005-2207.