



WHITE PAPER

Navigating A New Payments Landscape

***Fraud Prevention, Risk Management
and Regulatory Compliance***

October 2005





Executive Summary

Today there are significant changes in the payments industry. It is an era being defined by a declining volume of paper checks and associated revenue, and an increasing volume of electronic payments that provide less revenue. This shift brings to the forefront a need to re-address where the risks for payments fraud and expense exist, as well as what the current best practices are to protect against these risks.

Although the exact nature and timing of Check 21's impact on future check fraud remains in question, it is clear that check truncation and check destruction are creating new opportunities for fraud.

At the same time, the payments terrain is being impacted by other recent legislation, such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, and the Patriot Act. These are placing pressure on banks and corporations to improve their processes to better manage their risks.

This paper explores some areas of interest for banks and their corporate clients as they relate to fraud prevention, risk management, and regulatory compliance today.

Table of Contents

A Shifting Payments Landscape	3
Keeping an Eye on Payment Processing Fees	3
Anticipating Consolidation in the Check Processing Business	4
Perfecting Online Banking	4
Servicing the Corporate Client with Technology	5
Payments Fraud Today	6
Payments Fraud is Still On the Rise	6
Paper Check Fraud	7
Impact of Check 21 on Payments Fraud	8
ACH Debit Fraud	9
What are the Best Practices to Stem the Tide?	10
Your Corporate Clients Can Evaluate their Risks for Check Fraud	11
Managing the Risks	12
Navigating Legislative Impact and Compliance	12
Sarbanes-Oxley Act and Section 404 Requirements	12
Gramm-Leach-Bliley Act of 1999	13
USA Patriot Act	14
Conclusions	16
AP Technology Helps Banks and Businesses Meet the Demands	17
<i>Appendix A: AP Technology Special Report on Payments Fraud Statistics</i>	

A Shifting Payments Landscape

Over the past 6 years, the Federal Reserve has reported that check volumes have been in steady decline. The 2004 Federal Reserve Payments study revealed another turning point in history where the number of electronic payments surpassed paper check payments. In 2003, the number of electronic payment transactions last totaled 44.5 billion — exceeding the number of checks paid, 36.7 billion.¹ The interesting fact is that check dollars are not declining at anywhere near the same rate as the number of checks paid.

In 2004, the ACH network accounted for more than 12 billion transactions, a 20% increase over 2003.² The growth in ACH payments is a rapid and marked change in payment behavior that presents a new fraud risk for both consumers and businesses — the risk of ACH debit fraud.³

It is agreed that paper checks will remain a major form of payment for businesses and consumers alike for a very long time, and that the risk for check fraud continues to rise annually despite declining check volumes. The annual dollar volume of checks remains high, indicating that higher dollar transactions are still taking place via the paper check. We may be approaching an environment where creating checks will require the level of controls used for wire transfers, simply because of the dollars involved.

Keeping an Eye on Payment Processing Fees

Payment behavior is changing, and it is due in part to the risks and fees associated with paper check payments. The 2005 Diamond Cluster Report, *Banking on Payments*, is an excellent resource on payments history and an educated perspective on where the industry is going.

http://www.diamondcluster.com/ideas/Viewpoint/PDF/ep_insight.pdf

The report explains that processing fees for various forms of payment will continue to be the driving force behind what forms of payment businesses will choose to accept and use.⁴

“If the cost of payment processing technology has declined and the volume of payments has soared, why haven’t banks reduced interchange fees?” These words from Daniel Olstad, Director of Payments at Best Buy Co. Inc, are being echoed by major retailers across the country. Wal-Mart along with other large businesses won a \$3 billion, precedent-setting lawsuit in 2003 against VISA and Mastercard over fee contentions.⁴

The increasing popularity of plastic payment adds fuel to the concern over interchange fees. Businesses pay the following average transaction processing fees on a \$100 purchase:

Signature Debit	\$1.12
Credit Card	\$1.87
PIN Debit	\$0.46 ⁴

Aside from retailers encouraging the use of PIN debit cards, they are also aggressively converting check payments to ACH at the point of sale (POS) to reduce their interchange fee overhead. The latest technology is creating a power shift from banks to businesses.⁴



Navigating a New Payments Landscape

© 2005 AP Technology. All rights reserved. AP Technology, SecurePay, SecurePayWEB, Transporter, fDX, SecureCheck, and SecureCheck RCP are trademarks of AP Technology. Transporter is a patent-pending technology.

With ARC conversion technology, businesses can continue to offer consumers the convenience of accepting checks but not incur the average \$3.00 processing cost. Businesses pay just pennies for an ACH payment.⁴ Conversion types include ARC, POP and RCK. Annual ARC volume alone grew by more than 1 billion payments and accounted for 54% of ACH growth in 2004.²

Businesses have also begun looking to companies like Debitman, which launched a national debit card POS network offering reduced processing fees in 2001. Debitman was inspired by a similar operation in Germany that processes half of the country's debit transactions with zero fees.⁴

Other companies take the path of trying to control their destiny with private label credit cards ...⁴

What does all this mean for banks? Bank revenue from consumer payments is now at risk. Lower-priced payments also leave little or no room for covering payment risks and any significant losses.

The future of transaction processing fees largely lies with what happens at the point of sale. Banks face a challenging future that is not entirely in their control, with emerging technologies that will affect the payments landscape in unexpected ways.⁴



Banks must find ways to effectively manage the competing silos they house to maximize bank revenue. The optimal collective path is not clear as it relates to products, services and pricing for their check processing, credit, debit and ATM units. Banks individually will need to develop global strategies for how their silos will work together to add value and reduce risks for businesses and their customers.⁴

Anticipating Consolidation of the Check Processing Business

With check volumes declining, the check processing business is ripe for consolidation among some of the largest banks and external players. Regional and small banks may decide Check 21 investments for processing any kind of check – electronic or paper - makes little sense. Some may opt for less expensive technology intended solely to accept electronic images and then outsource their paper check processing.⁴

Large banks, however, can actually consider making a profitable investment in Check 21 imaging and processing technology. Banks that can get large retailers to invest in imaging technology at the point of sale will reap the benefits of fewer touch points and costs associated with paper checks.⁴

Perfecting Online Banking

The growth of online banking is another obvious shift in the payments landscape. Consumers and businesses alike are finding the web a convenient vehicle for transactions, account reporting, and financial management. Balancing client information security and convenience has become a focus for all banks.



Banks are also now approaching next-generation online services where HTTPs is no longer considered secure enough for the services being rolled out. New secure transfer communications are being investigated and introduced.

Navigating a New Payments Landscape

Servicing the Corporate Client with Technology

Payments processing does account for up to 40% of all banking income.⁴ Another source of significant revenue for banks is generated from their treasury offering to corporate clients. Again technologies are emerging that enhance treasury products and services by making them easier to implement and more convenient to use. In a competitive marketplace, banks of all sizes are seeking the technologies that reduce bank and client risks associated with implementation and, in turn, increase revenue opportunities.

Until now, all customer-based reporting services have been relatively similar; new technology enhancements can improve the customer-bank relationship. Previously information was delivered to the desktop and possibly to programs like Excel; tomorrow's services will tie directly to the client's AR, AP and ERP systems. Failure to offer clients state-of-the-art information delivery will leave lesser banks in a non-competing position.

Payments Fraud Today

Payments Fraud is Still on the Rise

In this evolving payments landscape, one thing remains certain, criminals continue to find ways to profit from payment methods that leave room for fraud.

Just take a look at paper check fraud. It continues to rise despite declining check volumes. According to the latest statistics from the *2003 Nilson Report*, check fraud now costs U.S. businesses in excess of \$20 billion annually.⁵

According to the most recent *ABA Deposit Account Fraud Survey*, attempted check fraud rose by a sweeping 28% in 2003, with criminals attempting to cheat businesses out of \$5.5 billion (an increase of \$1 billion dollars from when the last survey was conducted in 2001).⁶

With respect to deposit accounts, ABA survey respondents indicated that identity theft was the leading threat against the industry, with check fraud being second, followed by the internet.⁶

The *AFP Payments Fraud and Control Survey*, dated March 2005, gave a revealing look at the types, frequency, and costs of payments fraud today. Of the 256 member organizations that responded to the survey, 55% indicated they had been victims of some type of payments fraud in 2004. Four out of five of these organizations indicated that their highest dollar fraud resulted from checks, as compared to 8% reporting credit cards caused their highest dollar fraud, and 5% reporting ACH debits.⁷

Checks remain the most likely vehicle for payment fraud attacks, with 94% of the organizations that reported fraud indicating that they had been victims of check fraud in 2004.⁷

Survey results also show that fraud comes at a high price. For organizations reporting fraud, the median dollar amount for all payments fraud was \$26,600.⁷

For more information on payments fraud see

[***Appendix A: AP Technology Special Report on Payments Fraud Statistics***](#)

Paper Check Fraud

Actually, the number of checks being issued is decreasing at a much slower rate than the number of checks being processed, which means that most check processing volume statistics do not give the full picture on the number of checks in circulation that are available to be acted upon fraudulently.⁸

The paper check continues to be a very popular form of payment, and this will not change any time in the near future. *"... check usage isn't expected to go away anytime soon. Check payments remain particularly popular in transactions between businesses. A survey released yesterday by the Association for Financial Professionals, a trade group, found that more than 75% of business-to-business transactions are made with paper checks."*



- Robin Sidel, The Wall Street Journal, October 28, 2004

The availability of low-cost desktop publishing software, printers, and copiers, in addition to pressures on banks to clear checks quickly, makes the paper check an easy target for criminals. The predominant types of check fraud affecting banks and their clients include forgery, NSFs, counterfeiting, closed accounts, kiting, stop payments, and alterations.

Paper Checks Rights and Rules

The question of who is liable for check fraud is spelled out legally in the Uniform Commercial Code (UCC). Most often courts determine that both the bank and their client share some level of liability for fraud losses.

- UCC3-105 addresses the requirements for banks and their clients to use “ordinary care” to prevent check fraud. This would involve implementing “reasonable commercial standards” that prevail in the area in which the person is located and the industry in which the person is engaged. This section of code does not require financial institutions to examine each item, if failure to examine does not violate the institutions proscribed procedures and those procedures are commonly used in the area.
- UCC 3-405 addresses “comparative negligence” and indicates that the fraud risk remains with the company, or employer, if the bank exercised “ordinary care” in processing the check.
- UCC 3-406 addresses “contributory negligence” and indicates that the fraud responsibility remains with the company if it fails to safeguard checks by a “reasonable commercial standard” (such as positive pay), and that the failure to safeguard contributes to the check fraud.
- UCC 4-406 addresses “reasonable promptness” and indicates that there is a period of time in which the customer is required to notify the bank of unauthorized signatures and/or alterations of their checks. 48 hours is currently the maximum time limit.⁹

Although open to judicial interpretation, businesses and banks alike should be fully aware of their rights and responsibilities with regards to check fraud as explained in the UCC.

Impact of Check 21 on Payments Fraud

We have had a long time to implement effective measures to prevent various forms of paper check fraud. Check imaging or electronification, however, opens a new frontier for fraudsters who will now try to access and alter digitized information.

The Check Clearing for the 21st Century Act (Check 21) took effect on October 28th, 2004. It allows banks, if they choose, to remove an original paper check from the check collection or return process and utilize a substitute check (Image Replacement Document – IRD) without delivering the original check. The purpose of Check 21 was to enhance the efficiency of check payments processing and clearing, and to prevent a recurrence of a payments bottleneck that occurred just after the September 11, 2001 terrorist attacks and shut down our nation's airline system.⁴

"Under a federal law that will take effect today, banks will have more leeway to process checks electronically, and this will translate to shorter or even nonexistent float times - the grace period between the time the check is written and when the money is debited from the account."

- Jennifer A. Kingson, New York Times, October 28, 2004

Check 21 will most likely decrease some types of fraud such as bad check-writing schemes that rely on lengthy float time.

However, the general consensus is that Check 21 will actually result in increased check fraud, for many reasons:

- Criminals may begin to focus on schemes that are closer to the time of presentment.
- Substitute checks are a new target for alteration or counterfeiting.
- Proposed bar code security and other potential security measures for the Check 21 environment have not been universally acknowledged or accepted.
- Security features that are present on paper checks are lost during scanning and so fraud detection becomes more difficult from the point of truncation. *Industry groups are pursuing "image-survivable" features. However, as of now, these are not available.*⁸
- Check 21 allows banks to decide how long to retain their paper checks after conversion, meaning that once the paper check is destroyed so is all evidence of counterfeiting, forgery and alteration. *This will likely become an issue in check fraud claims – when the key evidence of the crime is no longer available because it has been destroyed.*

*"Payments are going to be in an evolving environment that the world hasn't seen for quite some time" says Steve Hill, managing principal of the global payments consulting division at Carreker Corp. Hill believes that the Check 21 changes will bolster positive pay - the strongest protection against check fraud being employed by companies today.*¹⁰



Check 21 Rules and Rights

Checks processed through Check 21 technology may be disputed by businesses for only 30 days.⁴

ACH Debit Fraud

With ACH payments now surpassing paper check payments, everyone agrees that containing ACH fraud is a growing concern. The availability of low-cost software makes fraudulent ACH transactions readily possible for criminals.³

A party really only needs two pieces of information to initiate an ACH transaction, the routing number of the payor's bank and the payor's account number.³ In affect, a company without proper internal controls may remain unaware that a fraudulent debit has been made on their account for many months, and by current rules this may make it impossible for a company to regain lost funds.

There are three types of ACH payments that allow billers to originate ACH debits to *consumer* accounts using info from their check. At this time, this does not apply to *business* checks, but may likely apply in the near future. Also, the biller would not know if a criminal presented a stolen consumer or commercial check.¹¹

Much of the fraud problem seems to be stemming from ARC, WEB and TEL transactions:

- **ARC Electronic Check Conversion** – conversion of paper checks to ACH debits at a drop box or lock box. Fraud can occur if the contents of the lock or drop box fall into the wrong hands. In addition, the ability to determine a consumer check by anything but the physical length of the check has not been satisfactorily addressed.
- **TEL Telephone Authorizations** – one-time ACH debit transactions are initiated by phone. This creates the opportunity for fraud if the proper security is not in place. This risk is becoming more and more a risk for the depository institution; knowing your customer is critical, as always.
- **WEB Web-Initiated Transactions** – one-time or recurring ACH debits via the internet. These transactions undoubtedly do not meet the NACHA written-permission requirement, and are subject to fraud. This risk is becoming more and more a risk for the depository institution; knowing your customer is critical, as always. The ability to spot changes in your customers' payments behavior is key, as some new companies using the internet can run into such problems with fraud rather quickly.³

According to 2003 statistics, the aforementioned transactions carry a 14-17% payment rejection rate, as compared to a 2% rejection rate for more conventional business-to-business, consumer-to-business, or business-to-consumer transactions.³

ACH Rights and Rules

- NACHA's operating rules require that a payee have the formal written permission of the payor to initiate an ACH transaction. However, as bank's realize, this is a nearly impossible requirement to enforce, especially given the added difficulty that ACH is very likely to be initiated and run through a different bank from the payor.³

- According to ACH rules from NACHA, a company has 24 hours from the posting date to rescind an ACH debit from an account. Consumers have 60 days from the posting date.³

What are the Best Practices to Stem the Tide?

There are a number of defenses that banks should encourage their corporate clients to implement to combat check, ACH and other forms of payments fraud. The *AFP Payments Fraud and Control Survey* makes it clear that larger organizations are much more likely to have implemented these techniques than smaller organizations. 88% of the organizations surveyed have already taken the step to implement positive pay or reverse positive pay, and 71% use ACH debit blocks of some kind.⁷

Following is a valuable checklist of today's best practices that will reduce any organization's exposure to check and ACH fraud:

- ✓ Reconcile your accounts daily for ACH and check activity.
- ✓ Keep ACH debit activity in a single and separate account. Separating ACH from paper disbursements allows for more timely and focused review of ACH activity.
- ✓ Add a "Post No Checks" restriction on electronic payment accounts.
- ✓ Use a post no debits on depository or zero balance accounts for deposits.
- ✓ Separate disbursement and reconciliation duties.
- ✓ Change the passwords regardless how much everyone complains and eliminate sticky notes with key passwords and control information.
- ✓ Have dual security administrators for electronic payments systems.
- ✓ Control access to payments processing areas.
- ✓ Replace employee paychecks with electronic or card payments.
- ✓ Use Positive Pay, Payee Positive Pay, or Reverse Positive Pay.
- ✓ Add ACH Debit Blocks or Filters. An ACH Debit Block will block all ACH debits from posting to that account. ACH Filters will only allow pre-authorized one-time or recurring ACH debits to post to an account.
- ✓ Use ACH Positive Pay. Companies using this service send a file to the bank with the names of trading partners authorized to initiate ACH transactions against their accounts. The bank matches the identities of those attempting to debit an account with those on the list provided by the company, and exceptions are reported to the customer to review before payment.
- ✓ Use Combined Check and ACH Reconciliation. This service is available at banks that have linked their check and ACH systems to allow ACH debits to be verified by the bank's positive pay service.
- ✓ Discuss check destruction policies with your bank and understand potential ramifications.
- ✓ Understand your bank's imaging system.
- ✓ Make yourself knowledgeable of any changes to check stock security features. There are industry groups right now working to find image-survivable features that will be incorporated into security check stock in the future to help prevent fraud in a post-Check 21 world.
- ✓ Perform a detailed risk assessment of your organization that examines your internal controls for fraud prevention and determines what technologies and procedures should be implemented for improvement. Make sure that you have (improved!) coverage when there are vacations and turnover.^{7, 8, 12}

Your Corporate Clients Can Evaluate Their Risks for Check Fraud

Banking clients are welcome to take a **Check Fraud Risk Assessment** by visiting <http://www.acuprint.com/for/cfra/> to receive a quick overview of their organization's strengths and weaknesses with regards to check fraud prevention planning.

Managing the Risks

Navigating Legislative Impact and Compliance



To comply with recent legislation, public companies and/or banks have been reviewing and documenting their processes to assure the accuracy, security and privacy of their information. The effort to comply can be a harrowing undertaking, and the path is not defined with exactness, but the end result will likely be a reduced risk for fraud. Following is a top-level overview of the most recent laws, outside of Check 21, along with a general explanation of their impact on banks and businesses.

Sarbanes-Oxley Act and Section 404 Requirements

Sarbanes-Oxley (SOX) legislation was enacted in July 2002 to regulate financial practice and corporate governance with stringent rules designed *"to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws. It is also meant to "deter and punish corporate and accounting fraud and corruption, ensure justice for wrongdoers, and protect the interests of workers and shareholders."* - President Bush¹³

The Sarbanes-Oxley Act, named after its creators, Senator Paul Sarbanes and Representative Michael Oxley, was prompted in large part by a series of high-profile scandals, like Enron. The Act is comprised of eleven segments. However, Sarbanes Oxley Section 404, "Management Assessment of Internal Controls," seems to be raising the most concern as to how exactly to comply.¹³

In very quick summary, Section 404 requires:

- A company's annual report to contain an "internal control report."
 - The "internal control report" must:
 - state management's responsibility for establishing and maintaining adequate "internal control" policies and procedures for financial reporting
 - and*
 - contain an annual assessment of the effectiveness of the "internal control" policies and procedures for financial reporting.
- Each company's auditor shall attest to – report on – the assessment made by the company's management.
- Each company must disclose whether it has adopted a code of ethics and requires prompt disclosure of any change to this code of ethics.¹⁴

Committee of Sponsoring Organizations (COSO) Enterprise Risk Management Framework

SOX compliance requires aligning a company's personnel and operations with the key components of the Enterprise Risk Management Framework (ERM Framework). The Committee of Sponsoring Organizations (COSO) of the Treadway Commission has recently released (Sept. '04) their final ERM Framework report that has become recognized by the SEC as the critical methodology for Sarbanes-Oxley Section 404 compliance.¹⁵

Quotes from Jerry Rehfuss, a Finance Director at Kimberly-Clark, when asked in July 2003 about SOX requirements:

"In other words, CEOs and chief financial officers who are signing off on the validity of data must be sure that the systems maintaining that data are secure. If their systems aren't secure, then their internal controls are questionable and those executives could face criminal penalties if a breach is detected. Perhaps this presents another good thing about the Sarbanes-Oxley Act: Security technology is no longer just an IT matter; it's an organizational and an integrity issue to be reckoned with at the executive level."

"I am not adverse to doing work, but this was one of the biggest pieces of corporate regulation that's come in decades," says Rehfuss

"You cannot have compliance without ensuring, through technological means, that the integrity of the corporation's financial records is intact. The internal controls mandated by Sarbanes-Oxley call for a strict set of access controls to be put into place that regulates who has access to what information."

The Sarbanes-Oxley Act puts in the foreground the need for companies to have mechanisms in place that assure security with regards to IT transmissions and accounting. The language of SOX issues in a new age of responsible and accountable practices that will help to prevent fraud.

To reiterate, it is not just about companies implementing best practices, but about creating accountability through our court system if companies fail to proactively seek out and implement the practices and solutions that could have prevented security breaches.

The way to comply with SOX remains vague and is a topic of current discussion, but clearly any solution will meld internal security practices with best-of-breed technology. SOX raises the bar for all public companies by requiring accountability, reporting that accountability, and the safeguarding of information integrity.

Gramm-Leach-Bliley Act of 1999

Senator Phil Gramm, Chairman of the Senate Committee on Banking, Housing and Urban Affairs, issued the following statement regarding the Gramm-Leach-Bliley Act:

"I believe we have passed what will prove to be the most important banking bill in 60 years. It overturns the key provision of the Glass-Steagall Act that divided the American financial system."

"Finally, we met the legitimate privacy needs of Americans by guaranteeing that every bank must tell every customer what its privacy policy is, by assuring that every customer can opt out by changing to another bank, if they don't like how they are treated, and by requiring that any bank which is considering use of our private information outside the institution give us an absolute right to simply say 'no.' This is the strongest privacy policy provided in American history, but also one that will not destroy the information age before it begins."¹⁶

Title V of the Gramm-Leach-Bliley Act addresses how banks must protect the privacy of customer information:

- Requires clear disclosure by all financial institutions of their privacy policy regarding the sharing of non-public personal information with both affiliates and third parties.
- Requires a notice to consumers and an opportunity to "opt-out" of sharing of non-public personal information with nonaffiliated third parties subject to certain limited exceptions.
- Addresses a potential imbalance between the treatment of large financial services conglomerates and small banks by including an exception, subject to strict controls, for joint marketing arrangements between financial institutions.
- Clarifies that the disclosure of a financial institution's privacy policy is required to take place at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship.
- Provides for a separate rather than joint rulemaking to carry out the purposes of the subtitle; the relevant agencies are directed, however, to consult and coordinate with one another for purposes of assuring to the maximum extent possible that the regulations that each prescribes are consistent and comparable with those prescribed by the other agencies.¹⁶

The Act requires all financial institutions, regardless of whether they form an FHC, to disclose to customers their policies and practices for protecting the privacy of non-public personal information. The disclosure, which customers would receive at the time of establishing the relationship and at least annually thereafter, would allow customers to "opt-out" of information sharing arrangements with non-affiliated third parties. The Act does permit financial institutions to share personal customer information with affiliates within a holding company.¹⁶

It is considered a criminal offense for any person (including firm employees) to obtain or attempt to attain customer information relating to another person from any financial institution by making a false or fraudulent statement to an employee of that financial institution.¹⁶

No. Section 313.12 generally prohibits disclosure of credit card, deposit, or other transaction account numbers "for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer."¹⁶

Financial institutions are already largely compliant with the requirements of this Act.

USA Patriot Act

As the Patriot Act was passed on October 26, 2001 there was a focus on securing U.S. funds from terrorism. By taking away the money that terrorists used, they would be unable to continue their activities in an organized manner. The end result has been an enhancement to overall account security and fraud prevention efforts.

The Patriot Act requires that financial institutions develop procedures to account for all relevant risks, including those presented by the types of accounts they offer, the various methods of opening accounts, the type of identifying information needed, and the financial institution's size, location, and type of business or customer base. Thus, specific minimum requirements in the Act, such as the basic types of information to be obtained from each customer, are often supplemented with risk-based verification procedures to ensure that the financial institution has reasonable assurance of each customer's identity.

U.S. Attorney Johnny Sutton for the Western District of Texas, writes:

"Like all Americans, I hold dear our freedom from unwanted government intrusion into our private lives. As a people, we have always recognized that greater freedom may be accompanied by somewhat diminished security. As recent events have shown, terrorism poses a serious threat to both our security and freedom."

"The Patriot Act strikes a reasonable and sensible balance between freedom and security to meet the real dangers we face. The act provides the essential means we need to defend ourselves against terrorists while maintaining and protecting the civil and constitutional rights we cherish."

Conclusions

Banks and businesses are watching as the payments industry goes through a rapid transition, and the true industry leaders will be the ones that seek and define the best ways to parlay the risks and opportunities associated with these changes.

Electronic payments are replacing paper check payments, and it is agreed that interchange fees and POS technology will continue to be important factors guiding a shifting payments landscape. With a declining number of checks, but large check dollar volumes remaining, consolidation within the check processing industry is expected. Online banking for businesses and consumers alike will thrive, and the banks that strike the right chord with secure and convenient offerings will have the greatest success.

Banks and businesses today will implement proven technologies that:

- ✓ affect the speed, security and cost of transaction processing
- ✓ add ease and cost-efficiency to implementing bank products and services
- ✓ enhance fraud prevention
- ✓ increase bank revenues, reduce risks, and reduce expenses
- ✓ support compliance with the latest legislation

It is agreed that the increasing complexity of the payments industry has, if anything, created new opportunities for fraud. Both check fraud and electronic payments fraud are growing concerns. In most cases, the risk premium for fraud is not included in standard bank payments pricing.

Banks and businesses that implement the best internal practices and technologies for fraud prevention will be the ones that are prepared to effectively protect themselves from fraud and its liabilities.

AP Technology Helps Banks and Businesses Meet the Demands

Implementing appropriate technologies is an important part of Risk Management planning for banks and businesses. AP Technology solutions reduce the risk for check fraud and provide secure access to banking information for your corporate clients.

9 of 10 leading U.S. banks have positive pay partnerships with AP Technology. In fact, the SecurePay solution is the world's best-selling positive pay conversion and auto-transmission software available today.

AP solutions are also helping customers attain compliance with the latest legislative demands.

Positive Pay File Creation

- **SecurePay** – software for positive pay file conversion and transmission
- **SecurePayWEB** – a web-based service for positive pay file conversion

Improved Client Access and Web Usage

- **Transporter** – software for unattended, one click information requests, and improved secure data exchange with a bank's internet information reporting system. Improved security of file transfers using the latest FTP and FTP variations

Accelerated Client Implementation and Reduced Transcription

- **fDX** – software service for client file translation and transmission to and from banks

Check and Form Printing

- **SecureCheck nX²** – a software-hardware solution for secure and efficient MICR laser check/form printing
- **SecureCheck RCP** – a software-based solution designed for secure and efficient MICR laser check/form printing to local and remote sites via the Internet
- **ezSigner** – software solution that reduces the risk of managing check signatures

About AP Technology

For more than 15 years, AP Technology has developed and installed secure payment solutions for businesses and banks throughout North America. As a private California corporation founded in 1989 (as AcuPrint, Inc.), AP Technology pioneered the development of secure and cost-effective MICR laser check printing solutions. The company has emerged as a leading provider of innovative software and web-based technologies that connect banks with their business clients.

In 1998, the company introduced SecurePay, the first client-based, universally-compatible positive pay software solution for use with a bank's existing positive pay services. To date, over 2,000 copies of SecurePay have been installed.

In 2005, AP Technology released SecurePayWEB, an online positive pay file conversion service that allows business clients to rapidly implement their bank's positive pay services without installing any software.

Now all businesses, both large and small, can receive the risk management advantages of positive pay through several economical alternatives from AP Technology.

Navigating a New Payments Landscape

For more information, contact:

Donovan Perkins
SVP, Business Development
760-602-5423
donovan.perkins@aptechnology.com

John Cipriano
SVP, Financial Services
760-602-5427
john.cipriano@aptechnology.com

Corporate Headquarters Address

AP Technology
6359 Paseo Del Lago
Carlsbad, CA 92009
800-258-5901
www.aptechnology.com

References

1. "Electronic Payments Surpass Paper Checks" USA Today, posted 12/4/05, http://www.usatoday.com/money/industries/banking/2004-12-06-checks-eclipsed_x.htm
2. "Banks Ride ARC to Record Wave of ACH Payments in 2004," NACHA press release by Michael Herd, April 11, 2005.
3. "Cash Management Banking Tools, Part 1, What's New? ACH Fraud," by David L. Sauerma n & Les Corkill, *CFMA magazine*, January-February issue.
4. Diamond Cluster Report, "Banking on Payments" by Carl Hugener and Larry Lerner, 2005, http://www.diamondcluster.com/ideas/Viewpoint/PDF/ep_insight.pdf
5. 2003 Nilson Report.
6. **"2004 Deposit Account Fraud Survey Report", November 2004, www.aba.com**
7. "Payments Fraud and Control Survey" by the Association of Financial Professionals, March 2005.
8. "Criminals are still Finding Opportunities for Fraud", article by Robert Stasik, Executive Vice President Mellon Financial Group, June 2005.
9. UCC Uniform Commercial Code.
10. Treasury & Risk Management Express, October 26, 2004 Volume 3 Issue 19.
11. "ACH Debit Fraud is on the Rise" by Raquel S. Filipek , IT Audit, May 15, 2005.
12. "New Tools Help Manage ACH Fraud Risk," from Inside Treasury Management, Hibernia, 2005.
13. "Introduction to Sarbanes-Oxley," The Sarbanes-Oxley Act Community Forum, <http://www.sarbanes-oxley-forum.com/>
14. "Section 404: Management Assessment Of Internal Controls," http://www.aicpa.org/info/sarbanes_oxley_summary.htm
15. "SarbOx Compliance: Getting into the ERM Frame of Mind," by Ann Elizabeth Robinson, Ph.D. – Visage Solutions, November 14 2003, http://www.visagesolutions.com/pdf/ERM_Frame_of_Mind.pdf
16. "Information Regarding the Gramm-Leach-Bliley Act of 1999," from the U.S. Senate Committee on Banking, Housing and Urban Affairs website.
17. "U.S. Attorney: Patriot Act is a sensible way to keep us safe" from the Preserving Life & Liberty website, <http://www.lifeandliberty.gov/>