Your Business At Risk: Payments Fraud Awareness

May 13, 2008
Today’s Speakers:

**Warren Takacs** is Senior Vice President and Finance & Risk Manager in BB&T’s Payment Solutions Division and has almost 20 years’ experience in various sales, credit risk management and operations roles in banking. Warren will be the moderator for today’s session.

**Michael Eley, AAP** is Vice President and Treasury Management Product Manager for BB&T’s ACH and Wire Transfer solutions and has more than 20 years of experience in banking and treasury services management.

**Barbara McAllister** is Vice President and Treasury Management Product Manager for BB&T’s Account Reconciliation, Positive Pay and CD-Rom Imaging solutions and has 27 years’ experience in banking and financial services management.

**George Wyatt** is Vice President and Treasury Management Product Manager for BB&T’s Commercial Web Information Reporting and Transaction Portal and has more than 30 years’ experience in banking and financial services management.
Agenda

- Will fraud impact my business?
- Why is fraud so difficult to detect?
- What examples of fraud could I encounter?
- How can I minimize the risk of fraud for my business?
- What fraud prevention tools are available?
- Questions & Answers
Will fraud impact my business?

Polling Question

Last year, my company experienced:

1. Attempted payments fraud
2. Successful payments fraud, but no financial losses
3. Financial losses from payments fraud
4. No fraud attempts
5. Don’t know
TODAY, an estimated three out of four companies experience payments fraud or fraud attempts each year. The cost to U.S. banks, businesses and their customers totals billions of dollars, and the number of incidents continues to grow at an alarming rate.

According to the 2008 Payments Fraud & Control Survey by the Association of Financial Professionals, 71% of businesses surveyed experienced actual or attempted payments fraud in 2007. 31% of these businesses incurred financial losses from payments fraud, with a median loss of $13,900.
Fraud in Today’s Market

Even though check volumes are declining, checks continue to be the preferred target of thieves; 94% of all organizations that experienced attempted or actual payments fraud were victims of check fraud. Other targeted payment types for fraud include:

- ACH debits (26%)
- Corporate purchasing and credit cards (13%)
- Wire Transfer (3%)

Source: 2008 AFP Payments Fraud & Control Survey
Fraud in Today’s Market

Check Fraud:

- Types include:
  - Counterfeit checks, imprinted with organization’s MICR line but other business name
  - Altered payee names
  - Lost, stolen or counterfeit employee paychecks
  - Fraudulent checks returned by Positive Pay, then represented as ACH debits
- 17% of organizations that experience check fraud suffer a financial loss*
- Accounts payable, disbursement and payroll accounts were most subject to check fraud*
- Many organizations avoided losses by using bank-provided services*

Source: 2008 AFP Payments Fraud & Control Survey
Fraud in Today’s Market

ACH Fraud:

- 30% of organizations reporting payments fraud activity were victims of attempted or actual ACH payments fraud
- Among organizations incurring financial losses due to ACH fraud, reasons frequently cited included:
  - Failure to reconcile accounts or return fraudulent ACH debit in a timely basis (56%)
  - Failure to use ACH debit blocks or filters (50%)
  - Internal fraud (19%)

Source: 2008 AFP Payments Fraud & Control Survey
Fraud in Today’s Market

Card Payments Fraud

Among organizations victimized by card payments fraud:

- 82% experienced fraud as a result of accepting consumer credit cards
- 54% experienced financial losses; frequently, losses were from “card-not-present” transactions accepted over telephone or web
- 45% experienced attempted or actual card payments fraud from corporate card transactions
- Prepaid/gift cards are a new vehicle for fraud attacks:
  - Fraudulent checks, credit debit cards are used to purchase prepaid/gift cards, then
  - The prepaid/gift card is used to purchase merchandise

Source: 2007 AFP Payments Fraud Survey
Fraud in Today’s Market

Card Payments Fraud (cont.)

- TJX, parent company of TJ Maxx, disclosed a massive breach of cardholder data in early 2007
- Sensitive data on more than 45 million Visa® and MasterCard® customers was exposed
- TJX expects to incur costs of up to $256 million in investigation, legal fees and security enhancements
Why is fraud so difficult to detect?
Detecting Fraud

What makes fraud so prevalent and difficult to detect?

- Today’s technology heads the list. Criminals have ready access to inexpensive computers and scanning equipment, as well as off-the-shelf software and laser technology. With these resources, criminals produce high-quality fraudulent checks or fake identification.
- Criminals are constantly looking for new types of lucrative fraud.
- Fraud attempts are not always external to the company.
What examples of fraud might I encounter?
Companies must be alert to the following examples that may involve employees, merchants or vendors:

- Counterfeit checks, which include a replica of your company check with a scanned image of your logo, or a check from a fictitious company.
- Alterations of a legitimate check, including a forged signature or altered amount.
- Fraudulent electronic debits, including fraudulent instruction to initiate ACH debits for consumer payments received via Internet or telephone; checks returned for fraud that are in turn converted to an electronic transaction and presented through ACH; and other converted checks returned as fraudulent or unauthorized.
Common Types of Fraud

- Electronic debits or outbound wire transfers sent for fraudulent purposes.

- Consumer credit card fraudulent purchases, sent by Internet or telephone from “card not present” merchants or from merchants not validating the CVV2 number on the card for purchases; stored value cards or card numbers that are stolen and used to make purchases.
How can I minimize fraud within my business?
Polling Question

Which type of payments fraud do you believe poses the greatest threat to your business?

1. Check fraud
2. ACH or Wire fraud
3. Card payment fraud
4. Internal fraud by employees
5. Fraud resulting from unauthorized access to our computers
Suggested safeguards to reduce risk and minimize financial loss – YOUR EMPLOYEES

- Conduct complete background checks for prospective employees and require mandatory vacations.
- Implement dual control and separation of duties.
- Review internal controls and procedures.
- Perform frequent random audits of employees’ work activities.
- Restrict the number of authorized signers.
- Educate staff on phishing and social engineering scams.
Suggested safeguards to reduce risk and minimize financial loss – YOUR DOCUMENTS/SYSTEMS

- Protect your company’s firewalls and computers with current anti-virus and anti-spyware software.
- Limit or restrict employee access to essential systems and data.
- Use a larger font for check printing; prevent adding a payee by including asterisks (above, below and to the sides).
- Utilize check stock with security features.
- Shred or securely store confidential documents.
Suggested safeguards to reduce risk and minimize financial loss – YOUR DOCUMENTS/SYSTEMS

- Make sure your card processing systems and hardware are PCI (Payment Card industry) compliant
- PCI security standards are mandatory standards adopted by Visa, MasterCard, American Express® and Discover® applicable to all merchants and processors
- PCI requirements for firewalls, network security, encryption and protection of cardholder data
- See additional suggestions available at www.bbt.com/pci
Suggested safeguards to reduce risk and minimize financial loss – YOUR DOCUMENTS/SYSTEMS

- If your company accepts card payments at your website, consider using a Payments Gateway service

- With a typical Payments Gateway service
  - Cardholder data is stored in a secure and PCI compliant data center, and not on your company’s computers
  - Cardholder data is submitted through a secure gateway with multiple firewalls and blockers
  - Cardholder authentication services verify address and card code information submitted over the Internet against actual cardholder records
Suggested safeguards to reduce risk and minimize financial loss – YOUR PROCESSES

- Reconcile accounts at least daily, including outbound ACH and wire transfers.

- Ensure that blank check stock, signature stamps, facsimile signatures and card stock are stored in a secure environment with inventory control.

- Establish and review controls and limits for all payments and wire transfers.

- Report fraudulent or suspicious transactions promptly.
Suggested safeguards to reduce risk and minimize financial loss – YOUR PROCESSES

Polling Question

My company reviews activity on its commercial checking accounts

1. Several times a day
2. Once a day
3. Weekly
4. Monthly
5. No set schedule/don’t know
What fraud prevention and detection tools are available?
Strategic Approach to Fraud Detection

Solutions are available to assist you in fraud prevention, whether you need of more timely access to account information or you want to transition from checks to electronic or card payment solutions. Examples include:

- Online Access
- Event Notification
- Positive Pay
- CD-ROM Paid Check Imaging
- Integrated Payables
- Direct Deposit
- ACH Debit Block, Debit Filters and Positive Pay
- Payroll Card
Strategic Approach to Fraud Detection

Online Access:

- Utilize your bank’s information reporting system to gain real-time access to your account activity.
- Monitor your current-day and previous-day balances and your detailed transactions along with paid check images.
- Determine whether your bank’s system can establish appropriate entitlements for each user and set limits for ACH and wire transfers.

Positive Pay:

- Compare the check issue information that you send with the checks paid against your account (serial number and dollar amount).
- Review suspect checks provided to you by your bank’s information reporting system.
Strategic Approach to Fraud Mitigation

CD-ROM Paid Check Imaging:
- Storing old checks in a secure environment or shredding them is no longer a concern because images of your paid checks are provided on a CD-ROM each statement cycle

Integrated Payables:
- Pay suppliers, vendors and employees by initiating a single file of payment instructions to your bank
- These payments are initiated via ACH, wire transfer and checks on behalf of your organization

Direct Deposit:
- Deposit your employees’ pay directly into their personal checking or savings accounts at the financial institutions of their choice
- Expense reimbursement, pension payments, dividends and other payments can also be handled through Direct Deposit
Strategic Approach to Fraud Mitigation

**ACH Debit Block, Debit Filters and Positive Pay:**
- Manage ACH activity on your account
- A blanket ACH Debit Block will prevent any ACH debit from posting to an account
- ACH Account Block filtering or screening capabilities will allow only certain vendors (originators) to electronically debit your account
- A maximum dollar limit can be set for each originator
- Account Block Positive Pay provides the ability to disposition and authorize rejected Account Block entries that fail to match your authorization criteria

**Payroll Card:**
- Pay your employees on a reloadable debit card each payday
- There are no payroll checks to reconcile or lost or stolen checks to reissue
Real Life Examples
Questions & Closing Remarks
Thank you for participating today!

Contact Information
Please call 1-800-810-5625 to reach a BB&T Payments Consultant in your area.

Or, visit our website at http://www.bbt.com/bbt/business/solutions/default.html

Evaluation
You will receive a short webinar evaluation via email. Your feedback is very important to us!

Member FDIC