Beating the Card Fraudsters

NACHA
The Electronic Payments Association

PAYMENTS 2006

May 5, 2006

AVENUE B
Consulting Inc.

Two Sparrows Consulting

Agenda

- Industry Overview
- Fraud Impacts Banking in Many Ways
- Hottest Fraud Topics
  - Account-Based Theft
    - Identity Theft
    - Phishing
    - ACH fraud
  - Card-Based Theft
    - Skimming
    - Fraud-Related Chargebacks
- Fraud Detection and Prevention Tools
- Stakeholder Solutions
- Case Study
- Industry Best Practices for Risk Management
  - Financial Institutions
  - Merchants
  - Customers

About Two Sparrows Consulting

- Independent Consulting Firm
- Payments Specialists
- Credit Cards, Debit Cards, ACH, Internet Payments
- Chip Cards, Stored Value, Loyalty, Merchant Acquiring, Bill Payment, Electronic Banking
- Project Management
- Training
- Marketing and Business Development
- M&A Services

About Avenue B Consulting, Inc.

- Management consulting firm focusing on payment systems products, services, and technologies
- Founded in 2002
- Over 26 years payments consulting experience
- Focus on financial services industry and electronic transaction processing
- Services include business and strategic planning, new product development, product market validation, business and IT assessments, and competitive analyses

Industry Overview

- Fraud Statistics
  - More than 370,000 ATMs in the U.S. and more than $1 trillion in withdrawals each year. Debit account fraud (via ATM and EFTPOS) accounts for 13% of fraud, a 60% increase over the last 2 years. (Source: BAI TransPay Conference, May 3, 2005)
  - Average fraud losses for on-line merchants equal 1.8% of revenues in 2005. (Source: Cardinal Commerce)
  - 9.3 million Americans were affected by ID fraud in 2004 costing $53 Billion. Mean cost per fraud victim: $5,686. (Source: Javelin Research and Strategy)
  - 4.6% of Americans were affected by ID theft in 2005. (Source: FTC)

Fraud Impacts Banking in Many Ways

- Fraud
  - Defined: Funds lost, at least temporarily, due to criminal activity
  - Fraud results in a partially or completely uncollectible loss. Fraud statistics generally report occurrence, and therefore usually overstate uncollectible loss.
  - Loss can accrue to any party in the value chain, dictated by consumer protection laws (EFTA, TILA), card association rules, or bank account terms and conditions, which vary by transaction and account type:
    - PIN debit – loss due to skimming is nominally the cardholder's responsibility, unless the FI reimburses
    - Signature credit, debit, ACH – loss accrues to the merchant or initiator (CNP, MOTO) or to the issuer if properly authorized, usually not the cardholder
    - Fraudulent extension of credit due to identity theft – ultimately the issuer, though the account holder often must take extreme measures to prove the fraud

Fraud Impacts Banking in Many Ways

- Fraud Impact
  - Non-PIN, card-based fraud historically runs at 6-7 basis points on dollar volume (Visa reported 6 bps for Q4 2005)
    - About 3% of interchange fees paid to issuers
    - According to Visa, 30% fraud losses are absorbed by merchants, 70% by issuers
  - PIN-debit fraud in 2004 stood at 0.3 basis point on dollar volume according to the Houston-based Pulse EFT network (Source: ATM & Debit News)
    - About 5% of interchange fees paid to issuers
    - Issuers and cardholders generally share the loss
    - This is a fast growing category, relative to others
  - Consumer perception of fraud and financial safety, sometimes influenced by consumer-protection groups, can be negatively impacted by high-profile breaches.
    - Recent PIN-debit breaches are alarming, effecting an estimated 600,000 cards. (Source: Gartner as reported in ATM & Debit News)
    - Several large issuers have re-issued cards in response

Fraud Impacts Banking in Many Ways

- Disputes and Exceptions
  - Defined: Transactions that are temporarily considered not final due to:
    - Actual fraud
    - Account-holder confusion and/or concern over potential fraud
    - NSF (ACH, check)
    - Error
    - Non-compliance
  - Disputes and exceptions require some level of intervention by some or all of the parties to a transaction
    - Account-holder discovery and dispute initiation, generally with their FI
    - FI dispute processing, in a manner dictated by EFTA, TILA, card association rules and their own policies
    - Merchant (if involved) providing proof of transaction and/or proof of rules compliance
  - Parties involved in the dispute pay their own processing and operations costs. Chargeback fees (associations and FIs) and NSF fees (FIs) are often assessed.

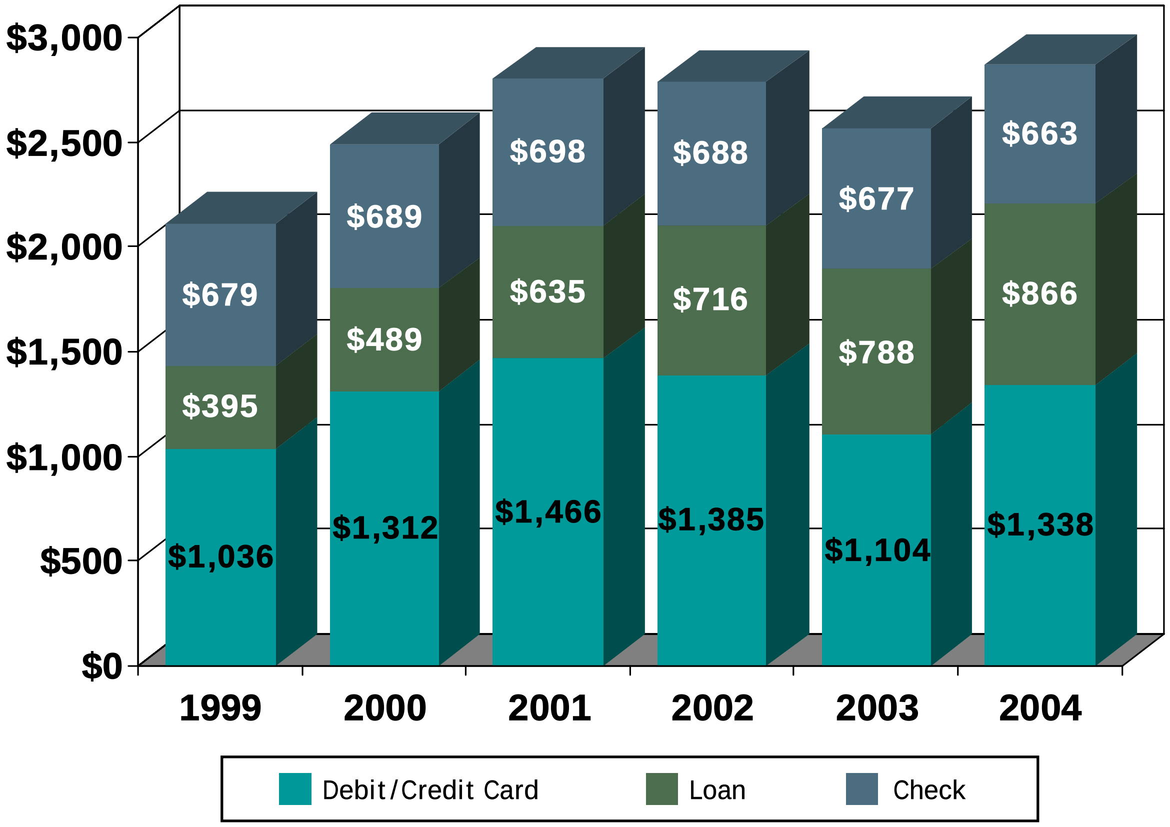
Fraud Impacts Banking in Many Ways

- Disputes and Exceptions Impact
  - Processing and operational costs related to resolving disputes/exceptions is significant: $10 - $50 per case for FIs
    - Even if only fraudulent transaction are considered, these costs are of the same order (or greater) than the uncollectible fraud loss itself
  - Costs accrue even for disputes/exceptions that are not a result of fraud
  - Statistics on dispute/exception rates are difficult to come by, though retail ACH entries are returned at a rate of about 1% (Source: Federal Reserve Bulletin, Spring 2005) much greater than the rate of actual fraud for the ACH.
  - Disputes resolved directly by issuers or merchants are not reported through the card associations
  - Bottom line: The cost to the banking industry of processing disputes and exceptions is likely *greater* than the losses due to fraud.

Risk management is about loss control and processing/operational cost control – reducing the latter can have a big a benefit

Driving Factors: Enduring but Changing Fraud Loss

Fraud Losses at Retail Banking Institutions (US$ Million)

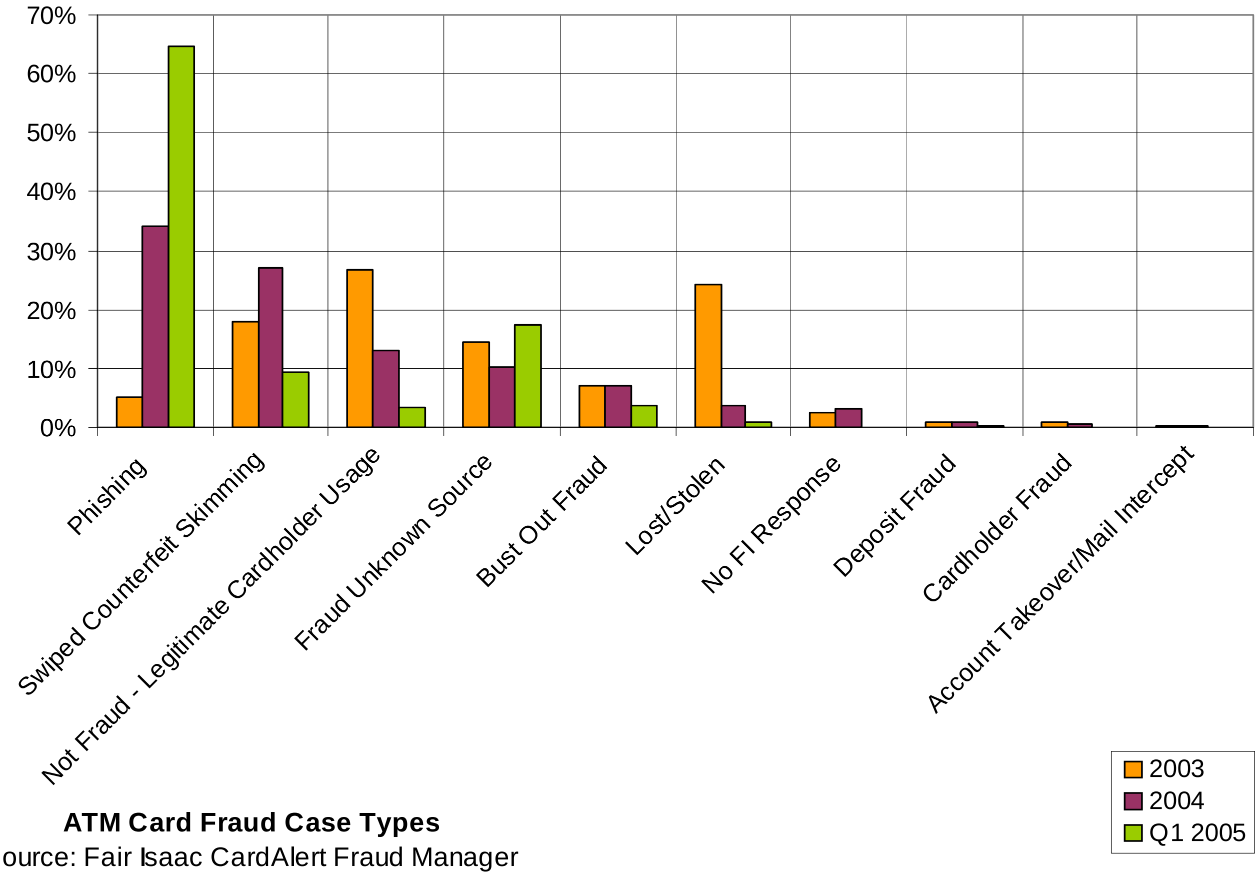


"The nature of fraud has been changing over the past few years. While over all losses from check fraud have been declining, new forms of fraud have risen, notably loan fraud, including mortgage fraud."

Source: Aite Group, LLC; Enterprise Fraud Management, From Silo Integration to BPO, May 2005.

Fraud Statistics

As percentage of total ATM fraud, Phishing and Skimming have been rising. Cardholder fraud is probably under-reported because merchants do not challenge it.



ATM Card Fraud Case Types

Source: Fair Isaac CardAlert Fraud Manager

Identity Theft

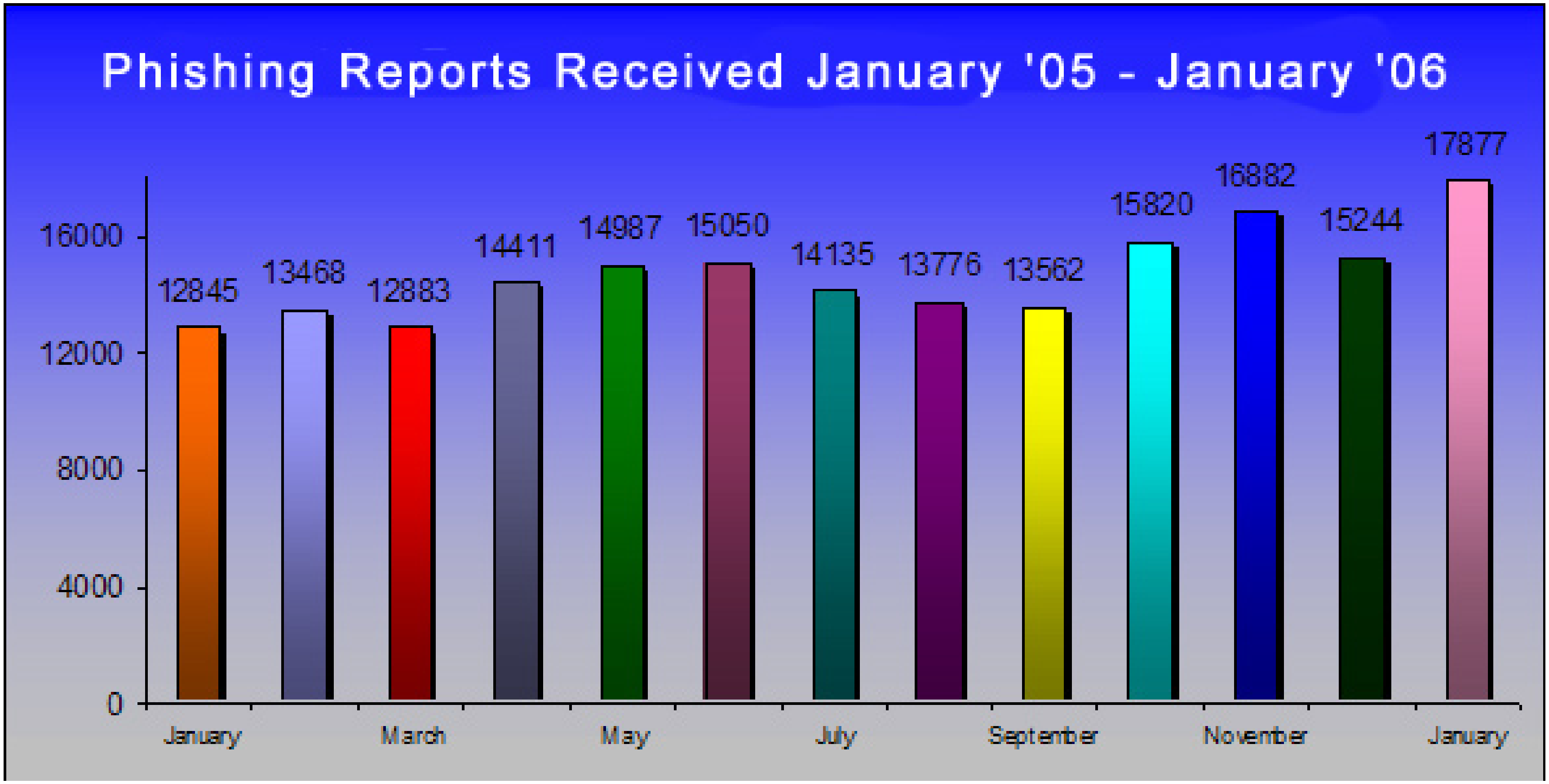
- Types of Identity Theft
  - New account fraud – using false identity to obtain credit card or loan; 60-80% is credit card loss
  - Payment fraud – use stolen information to pay for goods and services
  - Account takeover fraud – fraudster diverts cash via bill payment or funds transfer made on-line or at an ATM.
- Combating Identity Theft
  - Authenticating customers opening new accounts, ordering checks, reporting address changes
    - Techniques: Two forms of ID, database screening against known fraudsters, credit application scoring, checks for application inconsistency

Phishing – Account-Based Theft

- Definition: Account based theft perpetrated by replicating a legitimate financial institution's email or web site, tricking customer into divulging account numbers and passwords, and financial data; also mimic caller ID function on telephone.
- Challenge: Universal access to IP address; customers giving up confidential information
- Solutions:
  - Stronger authentication techniques (FFIEC)
    - Authentication of bank communications
    - Use secure email to authenticate all parties
    - Use of shared secrets (Corillian); photos as shared secrets (PassMark Security); intelligent authentication (combination of PC attributes & user behavior)
  - Encrypt and decrypt messages
  - Periodic scans of Internet to identify scam sites (NameProtect fraud detection services)
  - Customer education on securing confidential information

AVENUE B Consulting Inc.

Phishing – Account-Based Theft



Source: Anti-Phishing Work Group

Phishing – American Express Example

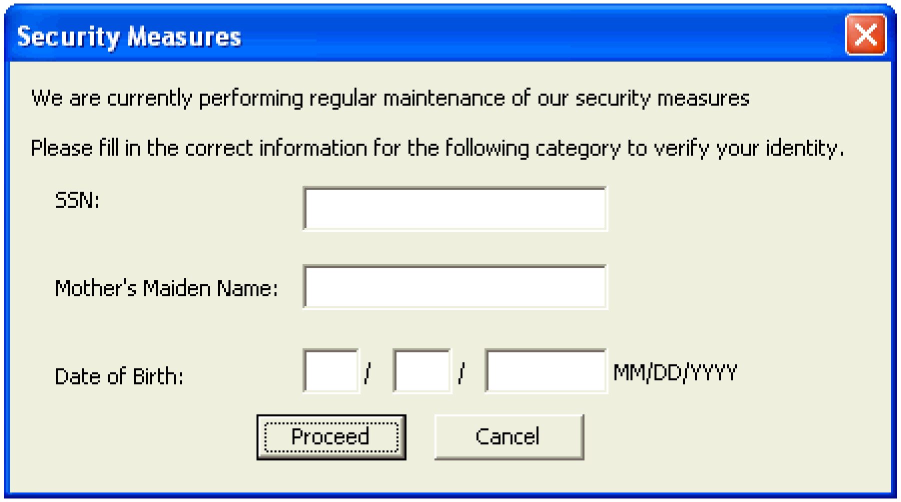
As an example of phishing, please note that some of our customers reported receiving the following pop-up screen while logged into our secure site. The pop-up screen is known to be a hoax and contains the following information:

Approximate date of the hoax: 3/29/2006 – present

Title of Pop-Up Box : Security Measures [see below]

Information Requested: Social Security Number, Mother's Maiden Name,

Date of Birth



Security Measures

We are currently performing regular maintenance of our security measures

Please fill in the correct information for the following category to verify your identity.

SSN:

Mother's Maiden Name:

Date of Birth: / / MM/DD/YYYY

Please note that this fraudulent activity may be the result of a computer virus and is not a part of the American Express website. If you received this pop-up box, your computer may have this virus.

Source: American Express website

ACH Fraud

- Definition: The use of unauthorized debits to DDA accounts.
- The Challenge: Losses due to new account funding via Internet, bank-to-bank transfers, bill payment and on-line purchases
- The Solution:
    - ACH fraud detection services that work like positive pay services
        - Review usual activity on accounts
        - Monitor suspicious telephone activity
        - Employ additional controls at new accounts desk
    - Network and Operator monitoring and early warning on unauthorized returns

Skimming – Card Based Fraud

- Definition: Copying fraudulent customer information on card magnetic stripe using a card reader, and then using the information to make counterfeit cards.
  - Often coupled with shoulder surfing, i.e., stealing PINs/passwords by viewing over the cardholder shoulder while entering such passwords
  - Also use overlay devices that imitate actual ATM devices
    - Card skimmers to capture card data (Lebanese Loop)
    - Fake PIN pads to capture PINs
    - Transmitter – to download the data.
- The Challenge: Difficulty identifying the point of compromise
- The Solution:
  - Review of DDA account daily withdrawal limits
  - PCI compliance regarding data storage
  - Use of host security modules
  - Involvement with financial institutions, card associations, networks and law enforcement

Fraud-Related Chargebacks – Card Based Fraud

- Definition: Card transactions that are disputed
  - Particularly impacting MOTO and Internet merchants
- The Challenge: Provide techniques to screen fraud while minimizing denying good customers
- The Solution:
  - Verified by Visa and MasterCard Secure Code automatic chargeback reason codes
    - Invalid T&E
    - Fraudulent MOTO/EC
    - Cardholder does not recognize
    - Non-cardholder authorization
  - Additional fraud screening measures, e.g., systems checks and manual reviews
  - Enhanced information on customer receipts

Fraud Detection and Prevention Tools

- Customer Authentication
  - Personal identification number (PIN)
  - Signature Capture / Digitized Signature
  - Address Verification Services: Verify Cardholder billing address against issuer file (MOTO)
  - Payer authentication programs: Verified by Visa & MasterCard Secure Card
  - Biometrics
  - Passive authentication solutions: IP geo-location and device fingerprinting
  - Two-Factor / Multi-Factor Authentication

Fraud Detection and Prevention Tools

- Card Verification
  - CVV & CVC 1&2
  - Card Alert Services – public hot card files, reduce/prevent losses from counterfeit cards
  - Chip-based Cards
- Transaction Authorization
  - Floor limits
  - Velocity files
    - Verification the co-location of subsequent transactions
    - Loyalty tie-ins
  - Rules-based engines
  - Neural network /pattern recognition - pattern recognition using verification of cardholder identification
  - Use of additional behavioral databases

Industry Best Practices

- ☑ Use card-based PIN offsets and validate offsets in authorization process
- ☑ Check CVV/CVC during authorization of PIN transactions CVC (CVC2 for Internet Transactions)
- ☑ Use neural network fraud detection system PRM
- ☑ Monitor CVV mismatch activity
- ☑ Report fraud to CardAlert Services
- ☑ Velocity Checking on bad PIN transactions
- ☑ Card activation process
- ☑ Confirm address changes
- ☑ Separate card and PIN mailers
- ☑ Don't use PIN for VRU or on-line banking

Source: First Data Corporation presented at EFTA Debit Card Security meeting, 2005.

Six Steps to Fight ATM Fraud

- Integrate siloed payments processing and fraud-management infrastructure
- Take an enterprise approach to data management across entire account and transaction lifecycles
- Integrate internal and external sources of data and analytics for real-time decisioning capabilities
- Invest in real-time solutions and flexible infrastructure through a trusted single provider of choice
- Automate back-office manual processes, then integrate them more effectively with front office ones
- When making changes, migrate operations gradually to mitigate cost; balance the risks and rewards of technology change

Source: eFunds Corporation presented at the ATM Operations Strategic Insights Forum.

Stakeholder Solutions

- Card Associations
  - Verified by Visa & MasterCard Secure Code
  - CVV-2 and CVC-2 – Card-not-present (MOTO) protection
  - PCI / CISP
- EFT Networks
  - Velocity checking and transaction scoring using neural networks
  - Card verification programs
  - Address verification services
  - PIN offset edits
  - Identity authentication and age verification
  - Searches in the Office of Foreign Assets Control database

Stakeholder Solutions

- Risk Management Software Vendors
    - Rules based engine doing multi-layer fraud checks, external (manual referrals)
    - Verify transactional integrity in real time and adjust authentication strength accordingly.
    - Risk-based authentication preventing online fraud through seamless integration with fraud detection systems.
    - Detection of fraudulent online activity and prevent illegitimate users from accessing accounts

- ATM and POS Hardware Vendors
    - Security devices designed to protect against skimming

Case Study – Massive PIN Hack

- Situation: Stolen debit card account numbers and PINs
  - Fraudsters create counterfeit cards “white plastic” and obtain PIN information from database.
  - Thousands of customer DDA accounts are compromised
  - Financial institutions banks needed to re-issue PIN debit cards after fraudulent activity is detected.
  - The most disturbing part of this hack is how the PINs were obtained. If they were stored by merchant, they are in direct violation of Card Association rules, and if so would be liable for all the of the fraud loses associated with those transactions.

Source: Financial IT Security, March 23 2006

Case Study – Massive PIN Hack

- What has been reported in the press - Fact vs. Myth?
  - ❑ "Retailers store PIN data on their databases."
  - ❑ "PIN data is readily accessible by hackers who can easily decrypt."
  - ❑ "PIN debit transactions are less secure than credit card."
  - ❑ "PIN is 'good enough'."
  - ❑ "Banks need to monitor ATM withdrawal limits across the DDA portfolio to limit skimming exposure."
  - ❑ "Customers can easily dispute PIN authorized transactions."
  - ❑ "Card based fraud is a serious threat to financial institutions."
  - ❑ "The re-issuance of cards cost more than the direct losses from the fraud."

Financial Institutions – Best Practices

- Continuous investment in new technologies and solutions to improve detection capabilities
  - Biometrics (e.g., fingerprinting) and digital signatures
  - Enhancements to neural networks
  - Profiling online banking patterns
  - Enhanced Internet security; Secure e-mail
  - Two/multi factor authentication for Internet purchases
- Develop enterprise-wide solutions around fraud initiatives and practices across the financial institution
  - Cross industry, coordinated efforts among check, credit card, debit, loan, and treasury departments
  - Evaluate new tools and technologies
  - Workflow management and real-time capture
- Quantify uncollectible fraud loss and customer support costs for disputed transactions to determine how they are impacting account and card-based profitability
  - Measure the ROI of investments in fraud detection and reduction
- Conduct periodic audits of fraud and risk management functions to uncover weak links in policies, processes, tools, and technology.

Merchant – Best Practices

- Continuous investment in new technologies and solutions to improve detection capabilities
  - ❑ Development of customer account profiles
  - ❑ Enhancements to neural networks
  - ❑ Enhanced Internet security; secure email
  - ❑ CVV-2 and CVC-2 for MOTO transactions
  - ❑ Address verification codes
  - ❑ Two/multi factor authentication for Internet purchases
  - ❑ Compare transaction authorization against merchant historical activity to detect suspicious cardholder activity
- Reduce disputed related costs
  - ❑ Prominently display policies concerning merchandise returns and refunds
  - ❑ Provide customer receipt data via email to Inform customers of transaction status (lower card-not-present fraud)
  - ❑ Print customer service information directly on the receipt, e.g., Web address and code for delivery status
- Quantify uncollectible fraud loss and customer support costs for disputed transactions to determine how their profitability by sales channel
- Conduct security compliance audits PCI compliance in the area of data storage
- Become certified according to e-Commerce Privacy and Security Standards

Customers – Best Practices

- Follow financial institution practices for creating PINs and passwords
- Follow financial institution policies regarding card and account safety
- Take reasonable precautions with identification information
- Visit financial institution webs sites often regarding emerging security threats
- Check accounts online periodically to review for unknown or suspicious transactions
- Frequently review financial statements
- Periodic review of credit bureau records for signs of unauthorized activity
- Buy a shredder!

Questions?

Paul Tomasofsky

Two Sparrows Consulting, LLC

(201)930-9551

ptomasofsky@optonline.net

www.twosparrowsconsulting.com

Maria Arminio

Avenue B Consulting, Inc.

(310) 540-5884

m.arminio@verizon.net

www.avenuebconsulting.com