"Be Better, Not Bitter"

Fraud Prevention Tactics for Credit & Debit Card Programs

ICBA BANCARD & TCM BANK

The Nation's Voice for Community Banks®

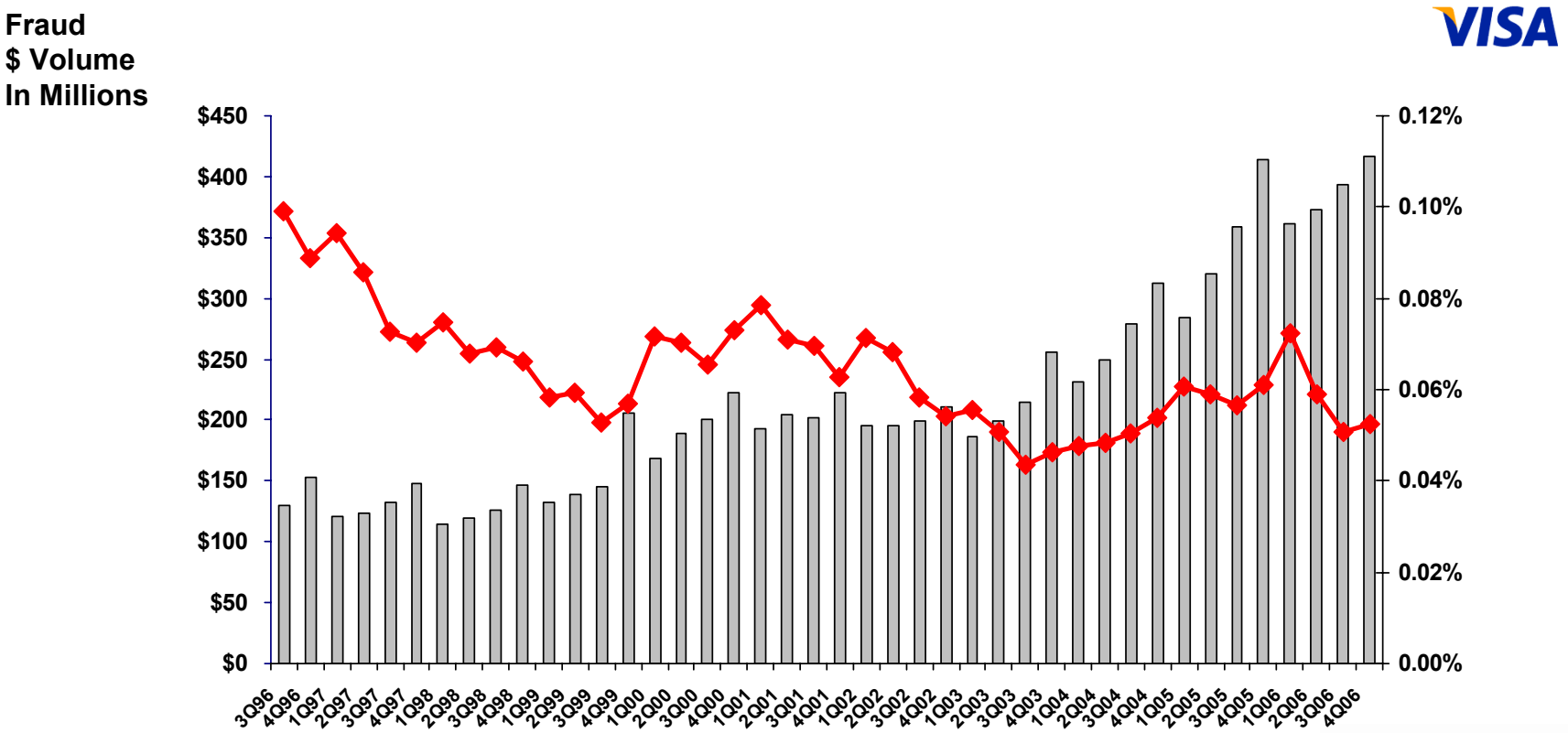
RIGHT SIZE SOLUTIONS FOR ANY SIZE BANK℠

Agenda

- **Industry Fraud Statistics for 2006**
- **Factors Contributing to Fraud**
- **Risk Management Trends**
  - **Long-Standing Risk Categories & Fraud Initiatives**
  - **New-Aged Fraud Trends**
- **Fraud Prevention Measures**
  - **Techniques**
  - **Monitoring**
  - **Patterns**
  - **Testing**
- **Current Industry Card Fraud**
- **FIS Card Fraud Initiatives**

ICBA BANCARD &TCM BANK

Industry Fraud Trends

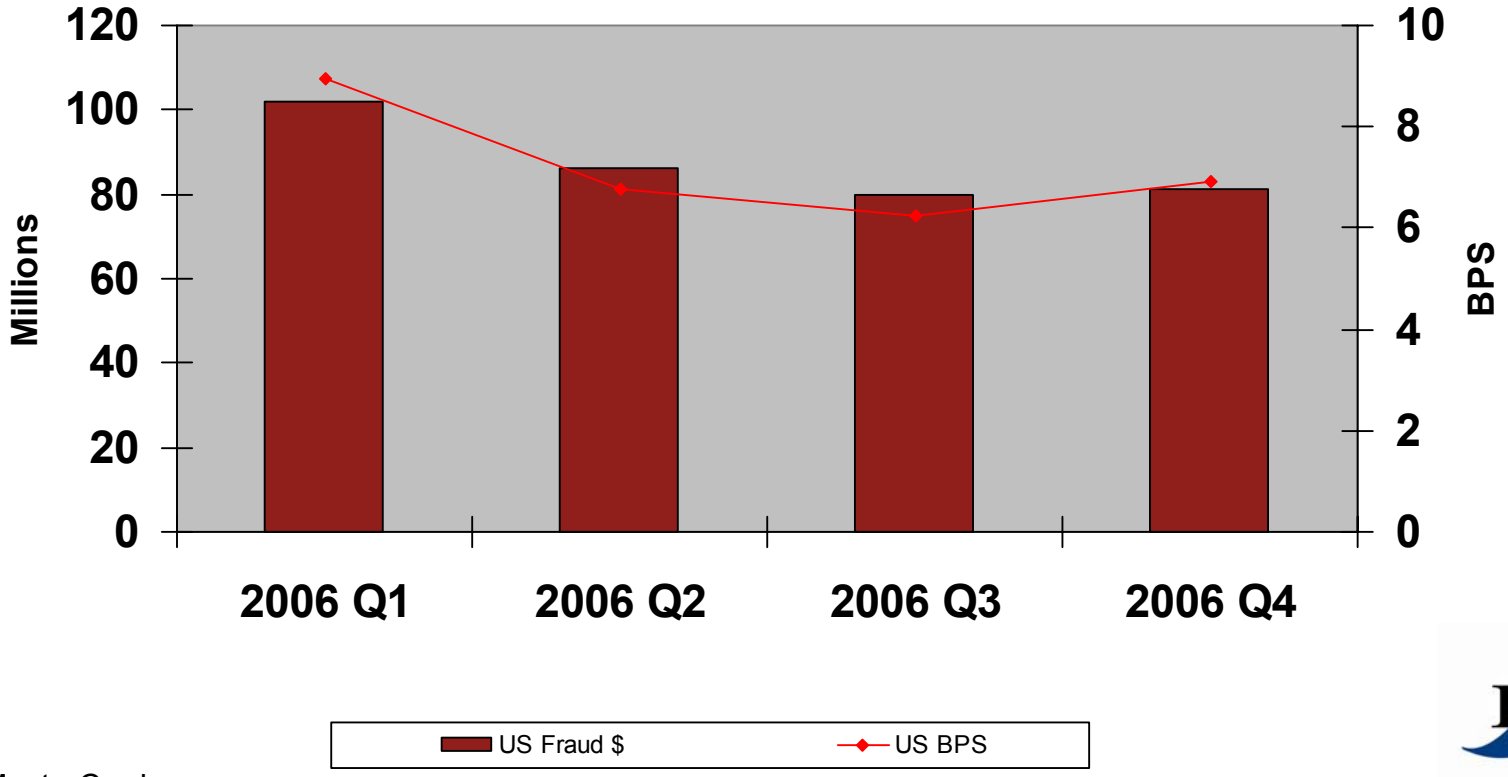


U.S. Issuing; All Products

Fraud $; Visa FRS. Net Fraud ratio; Member Operating Certificates(Visa BR&R)

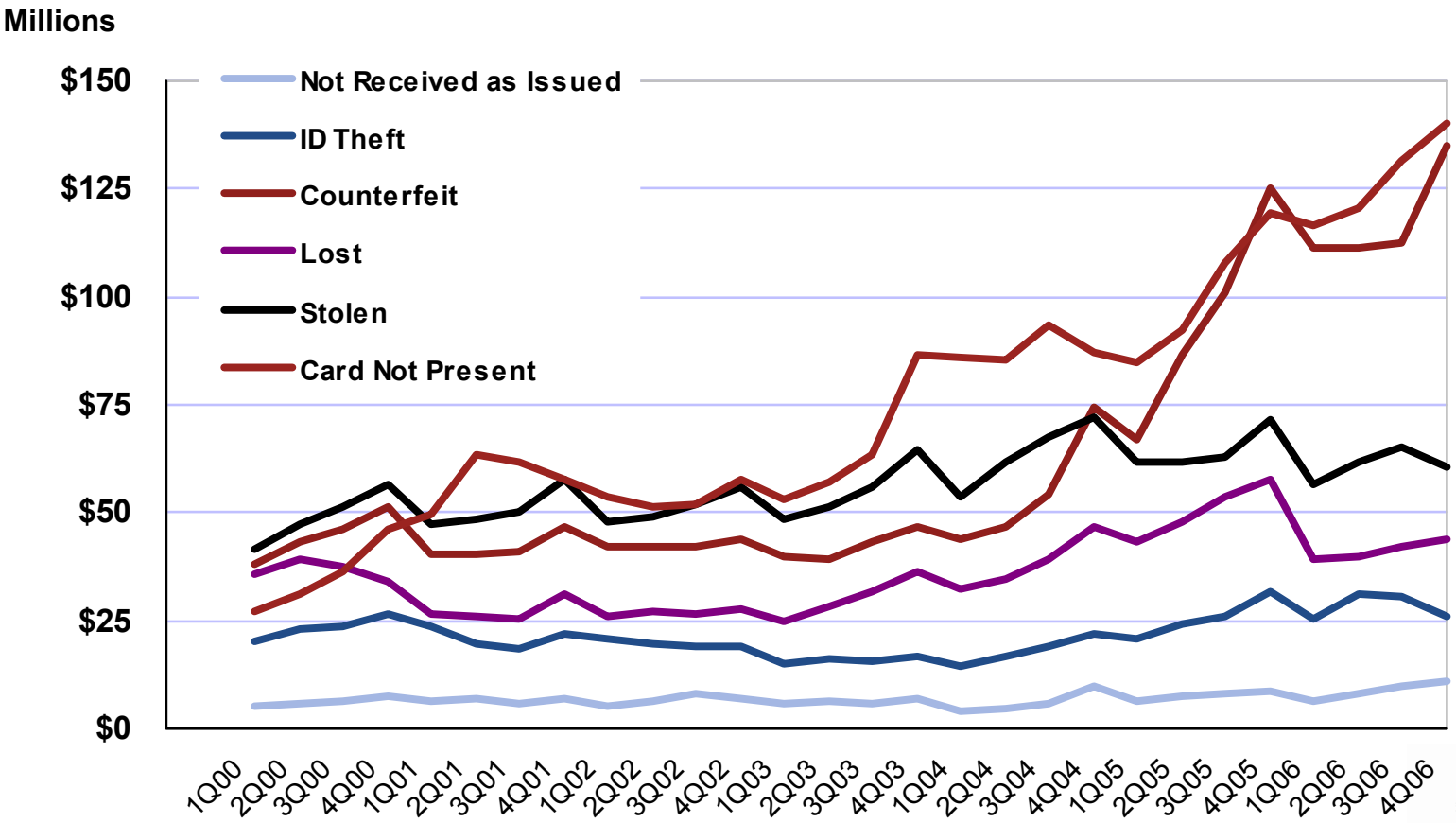
ICBA BANCARD &TCM BANK

US FRAUD EXPERIENCE



*MasterCard

U.S. Issuer Fraud Types



All Products

The Fraud Landscape

ATMs

Skimming
Phishing
Compromised ATM
Counterfeit

ID Theft
Deposit Fraud
Check Fraud

Branches

Merchants

Check Fraud
Card Fraud
Lost/Stolen
MOTO

Financial Institution

ID Theft
Deposit Fraud
Acct Takeover

Accounts

Phishing
Pharming
Hacking
ID Theft

Internet Banking

Counterfeit Checks

Check Processing

ID Theft
Vishing

Telephone Banking

ICBA
BANCARD
&TCM BANK

Current Fraud Environment

- Data Compromises continue to occur at increasing levels
  - Only a fraction reported
  - Estimates range from 20% to as little as 3% are made public
- Phishing has become more sophisticated
  - Financial Services continue to be the most targeted industry
  - Criminals are able to convince up to 5% of recipients to respond to their emails
- Identity Theft
  - 3.6 million households had at least one member as a victim of ID Theft in the preceding six months
  - 3 out of 4 consumers perceive ID Theft is increasing

ICBA BANCARD &TCM BANK

Current Fraud Environment

- Cyber crime is growing in diversity and sophistication
  - Internet provides a global network for exchange of knowledge and resources
- Criminal groups are professionally organized
  - Global in scope
  - Have been organized on the internet for years
  - Buying and selling stolen data in bulk
  - Taking advantage of weaknesses in payment applications, merchant inventory systems, accounting systems
  - They are also working together more than ever before

ICBA BANCARD &TCM BANK

Emerging Fraud Trends

- Professional Malware groups offering service
- Recruiting to popular teen chat rooms for individuals in Canada and the US to cash out dumps with PINs.
- Trojans delivered a maximum 2,000-5,000 installs per day at $40/1,000 installs.
- Collection of data being put into databases to run information against.

ICBA BANCARD &TCM BANK

Long-Standing Risk Categories
&
Fraud Initiatives

ICBA
BANCARD
&TCM BANK

Basic Fraud Categories

- Lost/stolen
- NRI (postal intercepts)
- Fraud application
- Account takeover
- Card not present (CNP)
- Counterfeit fraud
  - Skimming

ICBA BANCARD &TCM BANK

Existing Risk Management Category & Fraud Initiative By Type

- **NRI (Postal Intercepts)**
  - **Card Activation**
    - Authorization declined if card not activated
    - Activate if cardholder calls from home phone (ANI)
    - Last 4 digits of SSN
    - New accounts, reissues
    - Post mailer option
    - ANI added to Card Activation Report

ICBA BANCARD &TCM BANK

Existing Risk Management Category & Fraud Initiative By Type

- **FRAUD APPLICATION**
  - **Issuer's Clearinghouse Service (ICS)**
    - Approved and declined applications submitted
    - Fraud accounts submitted
    - ICS alerts received via reports
- **ACCOUNT TAKEOVER**
  - Change of address confirmation letters

ICBA BANCARD &TCM BANK

Existing Risk Management Category & Fraud Initiative By Type

- **CARD NOT PRESENT (MO/TO, Internet)**
  - **CVV2/CVC2**
    - Mismatches are declined
  - **Verified by Visa/MasterCard SecureCode**
    - Authenticate all internet requests from participating online merchants
  - **Address Verification Service**
    - Authorize exact AVS matches

ICBA BANCARD &TCM BANK

Existing Risk Management Category & Fraud Initiative By Type

- **COUNTERFEIT**
  - **CVV/CVC**
    - Encoded and validated on all magnetic stripe authorizations (Signature & PIN)
    - Mismatches are declined
  - **Authorization Name Matching (2005 Enhancement)**
    - Validated for all Track 1 authorizations
    - Mismatches are declined
  - **Expiration Date Matching**
    - Mismatches are declined

ICBA BANCARD &TCM BANK

Existing Risk Management Products & Services All Fraud Types

- **Falcon Alert Management**
  - All authorization platforms
  - Expert rule-writing
  - 24 x 7 servicing
  - Visa Advanced Authorization integration
  - Auto Dialer

ICBA BANCARD &TCM BANK

Existing Risk Management Products & Services All Fraud Types

- **Authorization Parameters**
  - Daily Limits – Velocity & Dollar Amount
  - Country Code Blocks
  - Merchant Code Blocks
  - Foreign Authorizations
  - ATM Authorizations
  - Overlimit Levels
  - PIN Validation
    - First Time at ATM
  - Credit Line Management Controls

ICBA BANCARD &TCM BANK

Existing Risk Management Products & Services ALL Fraud Types

- **Chargeback and Compliance - Recovery**
  - Chargebacks to merchants when applicable
  - Fraud reporting to Visa and MasterCard
  - Compliance processing
    - Any rule violation (outside of chargebacks)
    - Magnetic stripe violation filings against compromised merchants

ICBA BANCARD &TCM BANK

New-Aged Fraud Trends

ICBA
BANCARD
&TCM BANK

New-Aged Fraud Trends

- Internet Fraud
- Phishing schemes
- Voice Phishing – “Vishing”
- Counterfeit Skimming
- Data Compromises
- Identity Theft

ICBA BANCARD &TCM BANK

What Are The Criminals After?

- Criminal activities
  - Theft of card data
    - Account numbers
    - Full magnetic stripe data (CVV)
    - PINs
  - Personal Information
    - Name/address/dob/ssn
    - Mother's maiden name
  - Bot networks
    - Install mal-ware to PCs
    - Massive spam/phishing attacks

ICBA BANCARD &TCM BANK

Internet Fraud

ICBA
BANCARD
&TCM BANK

Internet Fraud

- Internet fraud permeates the industry
  - Computers are more accessible
  - Transactions occur in a card not present environment
  - Criminals remain anonymous
  - The Internet is both an innovator and a concealer

- Perpetrators of Internet Fraud
  - Savvy computer hackers
  - Organized crime rings
  - Teens and reclusive adults

ICBA BANCARD &TCM BANK

Federal Trade Commission Statistics

FTC top 10 Categories of Consumer Fraud Complaints -2003/2005		
Internet Auctions	15%	12%
Shop-at-Home/Catalog Sales	9%	8%
Internet Services and Computer Complaints	6%	5%
Prizes, Sweepstakes and Lotteries	5%	7%
Foreign Money Offers	4%	8%
Advance Fee Loans and Credit Protection	4%	2%
Telephone Services	3%	2%
Business Opportunities and Work-at-Home Plans	2%	2%
Magazine Buyers Clubs	1%	N/R
Office Supplies and Services	1%	N/R

ICBA BANCARD &TCM BANK

Internet Payment Methods

Payment Methods Used & Preferred Method of Payment for Online Purchases

Base: People that made online purchases in the past year

	Total (414)	Female (205)	Male (209)
Credit Card			
Used	82% avg	82%	83%
Preferred	68% avg	64%	71%
Checking/Debit Card			
Used	26% avg	30%	23%
Preferred	17% avg	19%	15%
Personal Check			
Used	18% avg	19%	18%
Preferred	9% avg		
Gift Certificate			
Used	5% avg	8%	3%
Preferred	1% avg	1%	1%
Money Order			
Used	4% avg	4%	4%
Preferred	0% avg	0%	0%

2005 Internet Fraud Watch

ICBA BANCARD &TCM BANK

Internet Fraud Prevention

- Monitor reports for excessive hand keyed and repeated low dollar authorizations
- Implement proper security systems for on-line banking products
- Develop policies that address Visa CAMS and MC Alerts
- Encourage cardholders to use secured web sites for transactions with credit and debit cards
- Promote Verified by Visa and MasterCard Secure Code

ICBA BANCARD &TCM BANK

Phishing

ICBA
BANCARD
&TCM BANK

PHISHING

What is Phishing?

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known financial institutions, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

ICBA BANCARD &TCM BANK

Phishing Email Schemes

- Unauthorized email solicitations to cardholders and consumers “phishing” for personal information
- False web-links are often built into the email scheme
- Mimic a legitimate and reputable company
- Create a plausible and persuasive premise
  - Account Alert
  - Update Your Information
  - Mandatory Password Change
- Require a quick response
- Promise security and/or privacy

ICBA BANCARD &TCM BANK

Phishing Email Schemes

- Increasingly committed by organized crime rings
- Growing rapidly around the globe
- Reputation and brand issues are at stake
- Schemes are affecting banks, credit unions, governmental agencies (IRS), payment providers, and auction services
- Phishing uses both social engineering and technical subterfuge

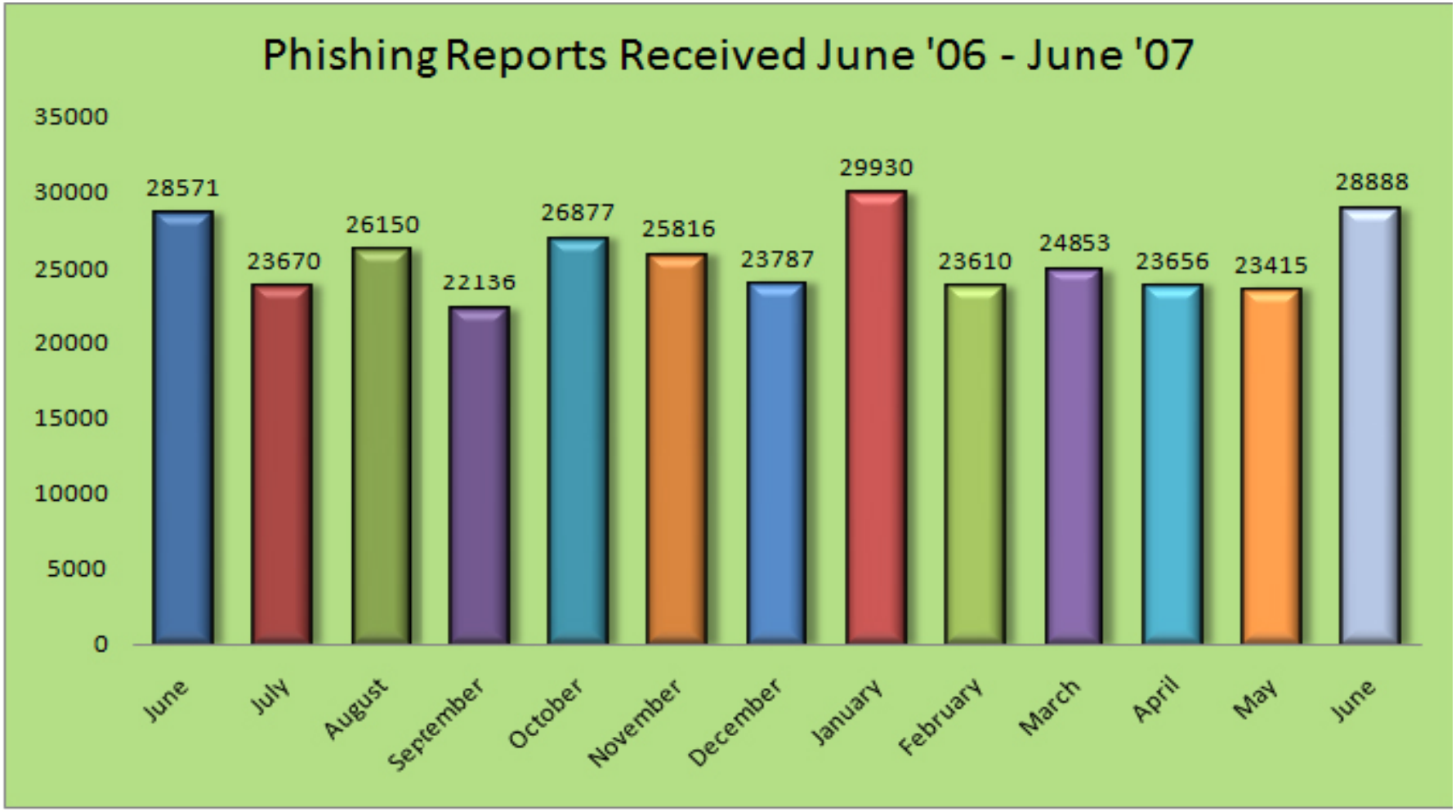
ICBA BANCARD &TCM BANK

Phishing

- Social Engineering
  - Use spoofing e-mails to lead consumers to counterfeit websites
  - Create an element of fear
  - Prey on public goodwill and compassion (Tsunami and 9/11 phishing schemes)
- Technical Subterfuge
  - Plant crime ware onto PC's to steal credentials directly.
  - Often use Trojans (viruses), key loggers, spy ware, etc.
  - Some phishing e-mails sneak key logger programs onto PCs by having user click on a link. Then when they go to their real FI's website the key logger will capture the log-in details and send them back to the fraudster

ICBA BANCARD &TCM BANK

Phishing Site Statistics



Source: APWG

Phishing

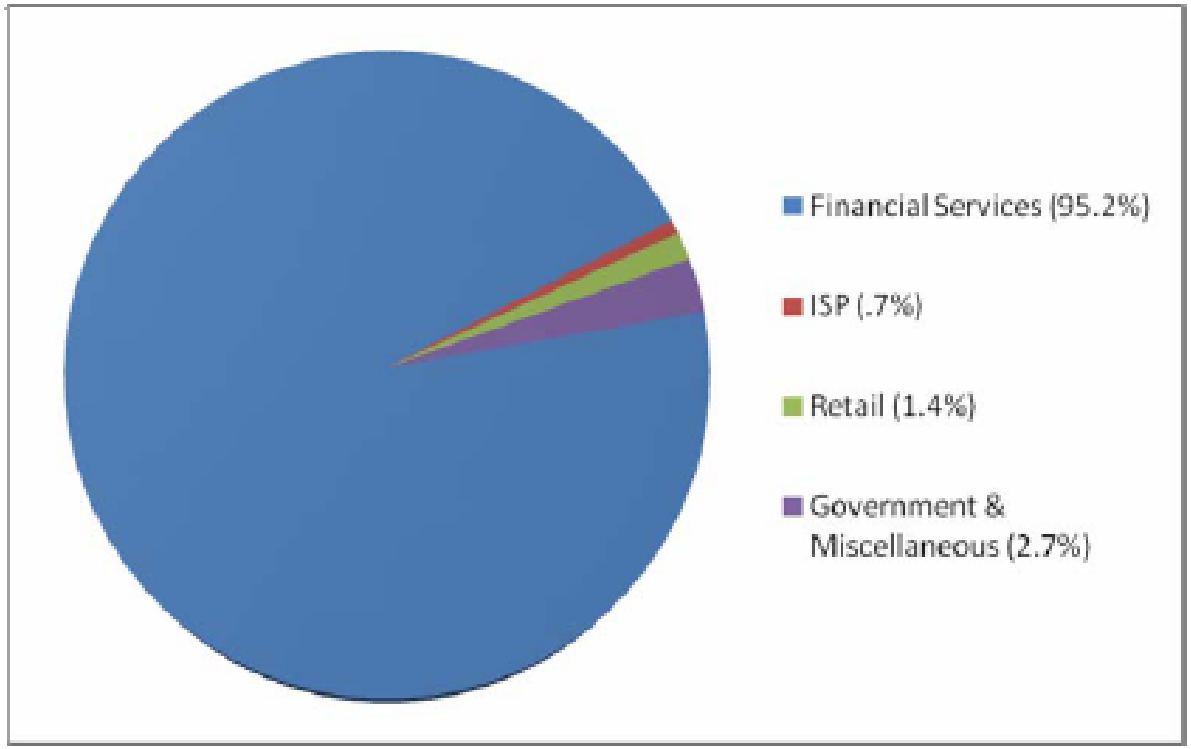
- Response rate for phishing scams is estimated at between 5% and 20%
- Financial losses stemming from phishing attacks have risen to more than $2.8 billion in 2006
- Average phishing website is online for 3.8 days
- Over 95% of all phishing attacks are targeted at the financial services industry (credit unions, insurance, ATM networks, and payment services)

ICBA BANCARD &TCM BANK

Phishing Statistics

Most Targeted Industry Sectors in June 2007

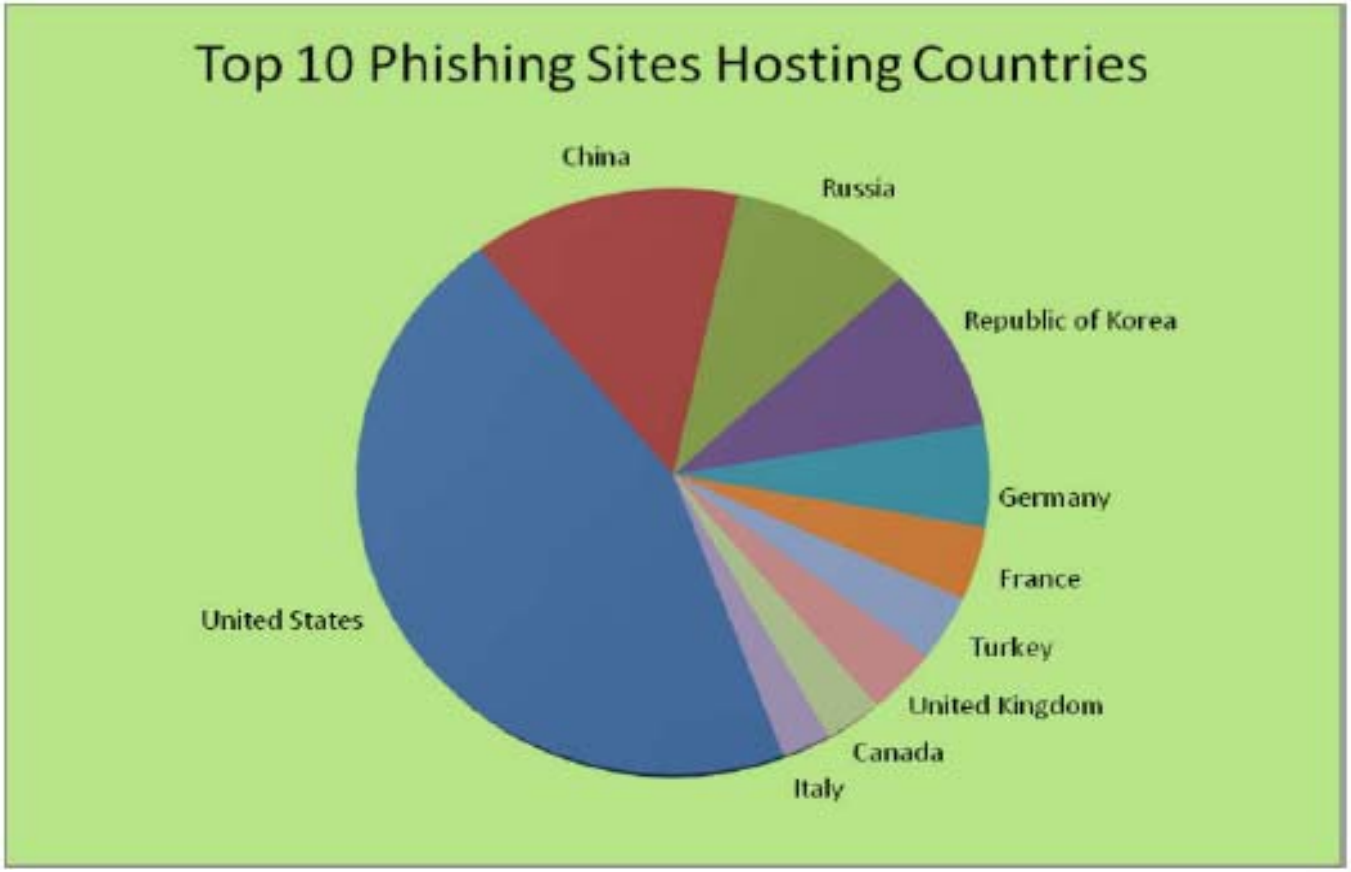
Financial Services continue to be the most targeted industry sector at 95.2% of all attacks in the month of June. APWG notes that US and UK tax authorities are being phished along with more social networking websites.



Source: APWG

Phishing Statistics

Countries Hosting Phishing Sites



Source: APWG

ICBA BANCARD &TCM BANK

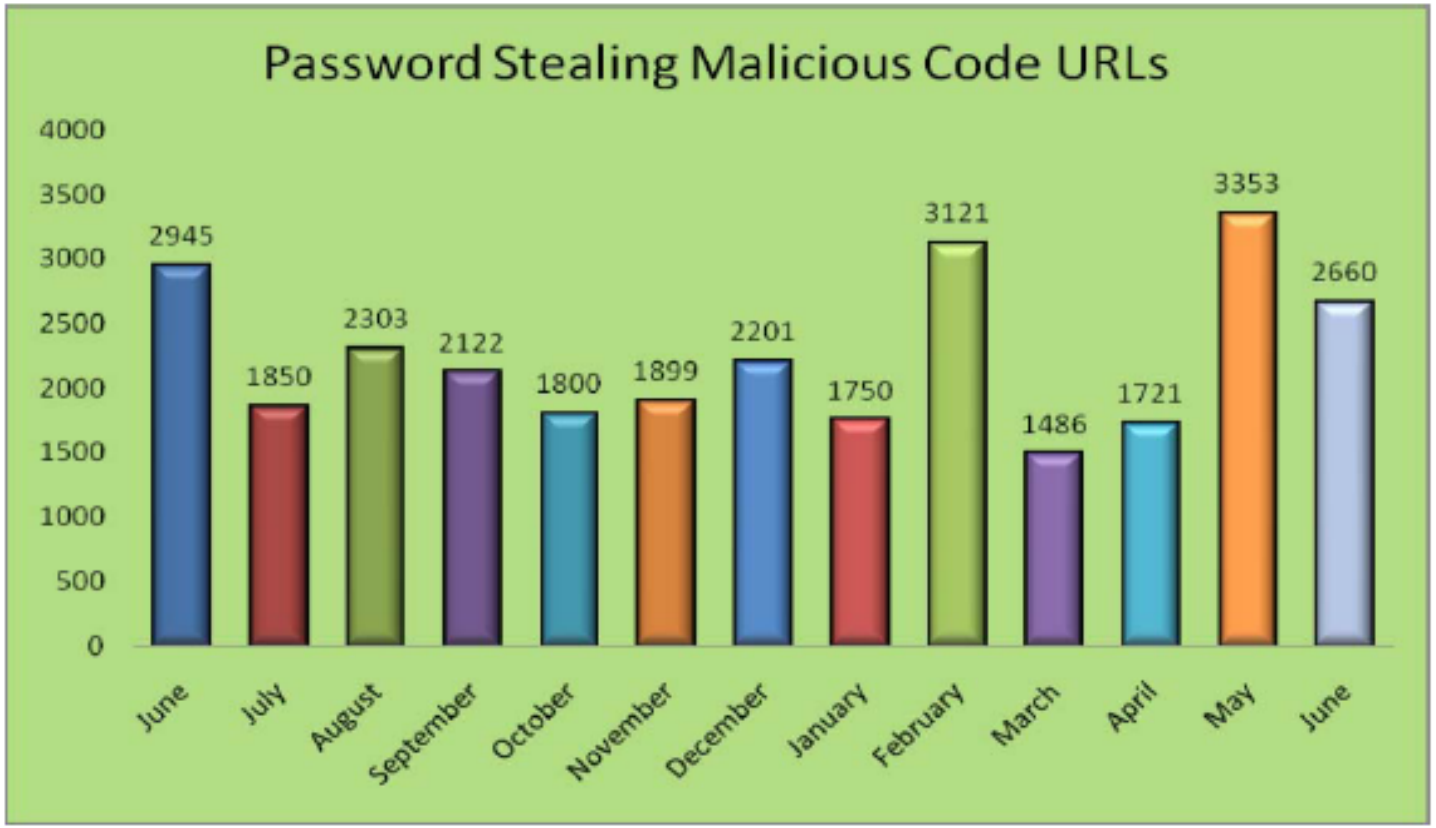
Phishing

- There has been a recent surge in password- stealing malicious-code URLs
  - Traditional phishing vs. directing individuals to click on a link
  - Clicking on the link downloads a Trojan Horse on the victim's computer
  - Will download keylogging software – keystroke capture
    - Once the consumer keys in a banking URL it will capture the User ID and passwords

FIS
FIDELITY NATIONAL INFORMATION SERVICES
&TCM BANK

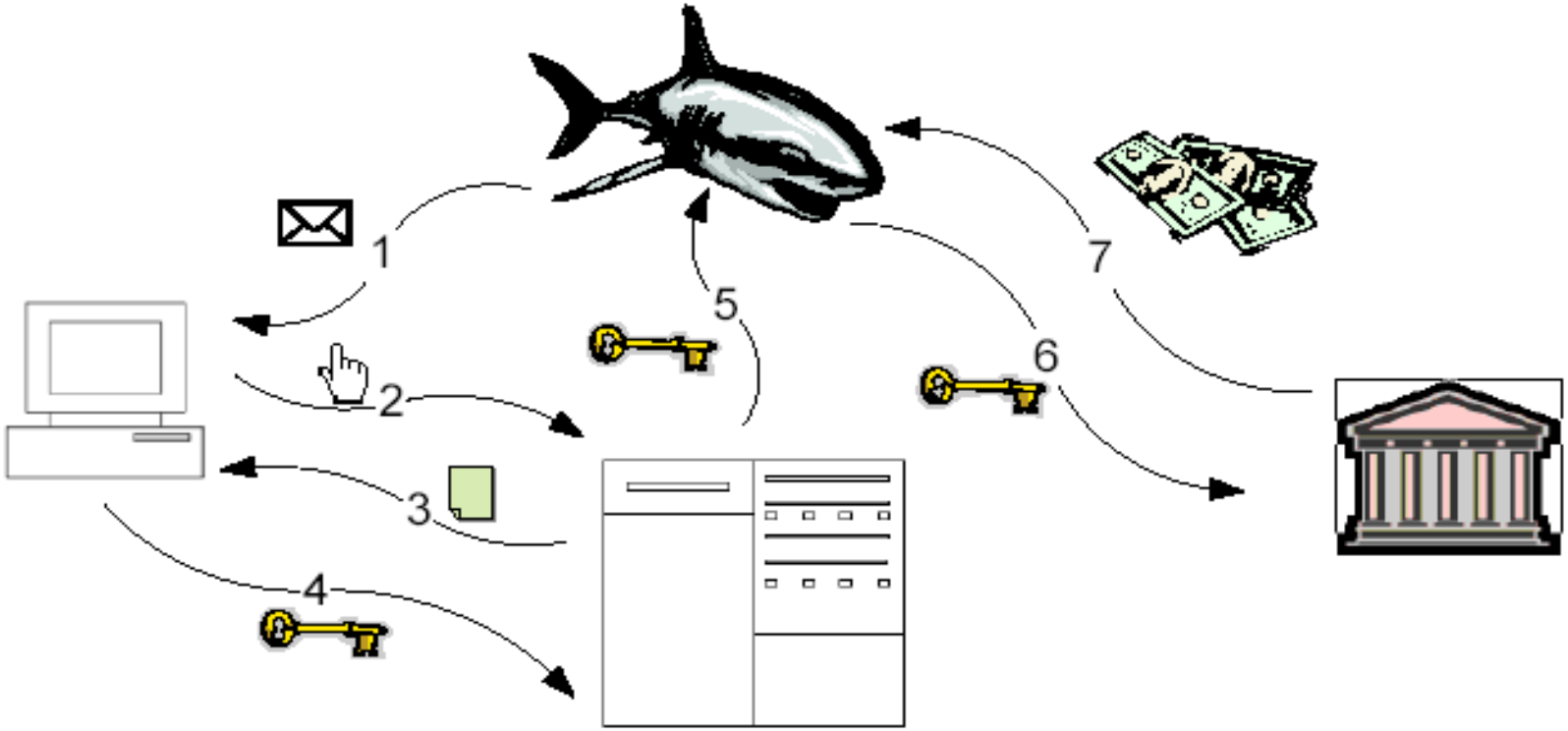
Phishing Site Statistics

Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers in June



Source: APWG

Steps in a Phishing Attack



Steps in a Phishing Attack

ICBA BANCARD &TCM BANK

Steps in a Phishing Attack

1. A malicious payload arrives through some propagation vector as a means by a deceptive email, an attachment to an email, downloaded software, or an exploit of a security vulnerability
2. The user takes action that makes him or her vulnerable to an information compromise such as clicking on a link or diverted to a fraudulent website
3. The user is prompted for confidential information
4. The user submits the information **(point of compromise)**
5. The compromised information is transmitted back to the phisher
6. The fraudster uses the compromised information to impersonate the user
7. The fraudulent party obtains illicit monetary gain, or otherwise engages in fraud using the compromised information

ICBA BANCARD &TCM BANK

Types of Phishing Attacks

- Phishing is perpetrated in many different ways
  - Deceptive Phishing
  - Malware-Based Phishing
  - Content-injection Phishing
  - Man-in-the-middle Phishing
  - Search Engine Phishing
  - DNS-Based Phishing (Pharming)
- Most dangerous phishing attacks are carried out by organized crime

ICBA BANCARD &TCM BANK

Deceptive Phishing

- In a typical scenario, a phisher sends deceptive email, in bulk, with a "call to action" that demands the recipient to clink on a link.
- Examples would include:
  - A statement that there is a problem with the recipient's account at a financial institution or other business.
  - A statement that the recipient's account is at risk, and offering to enroll the recipient in an anti-fraud program
  - A claim that a new service is being rolled out at a financial institution, and offering the recipient, as a current member

ICBA BANCARD &TCM BANK

Malware-based Phishing

- Malware-based phishing refers to generally to any type of phishing that involves running malicious software on the user's machine
- The most prevalent forms of Malware-Based Phishing are:
  - Key loggers and Screen loggers
  - Session Hijackers
  - Web Trojans
  - Hosts File Poisoning
  - System Reconfiguration Attacks
  - Data Theft

ICBA BANCARD &TCM BANK

Content-Injection Phishing

- Content-injection phishing refers to inserting malicious content into a legitimate site.
- The malicious content can redirect to other sites, install malware on a user's computer, or insert a frame of content that will redirect data to a phishing server

ICBA
BANCARD
&TCM BANK

Man-in-the-Middle Phishing

- Man-in-the-Middle phishing is a form of phishing in which the phisher positions himself between the user and the legitimate site.
- Messages intended for the legitimate site are passed to the phisher instead, who saves valuable information, passes the messages to the legitimate site, and forwards the responses back to the user.

ICBA BANCARD &TCM BANK

Man-in-the Middle Attack

Man-in-the-Middle Attack

Search Engine Phishing

- Phishers create a web page for fake products, get the pages indexed by search engines, and wait for users to enter their confidential information as part of an order, sign-up, or balance transfer
- Web pages typically offer products at a price slightly too good to be true

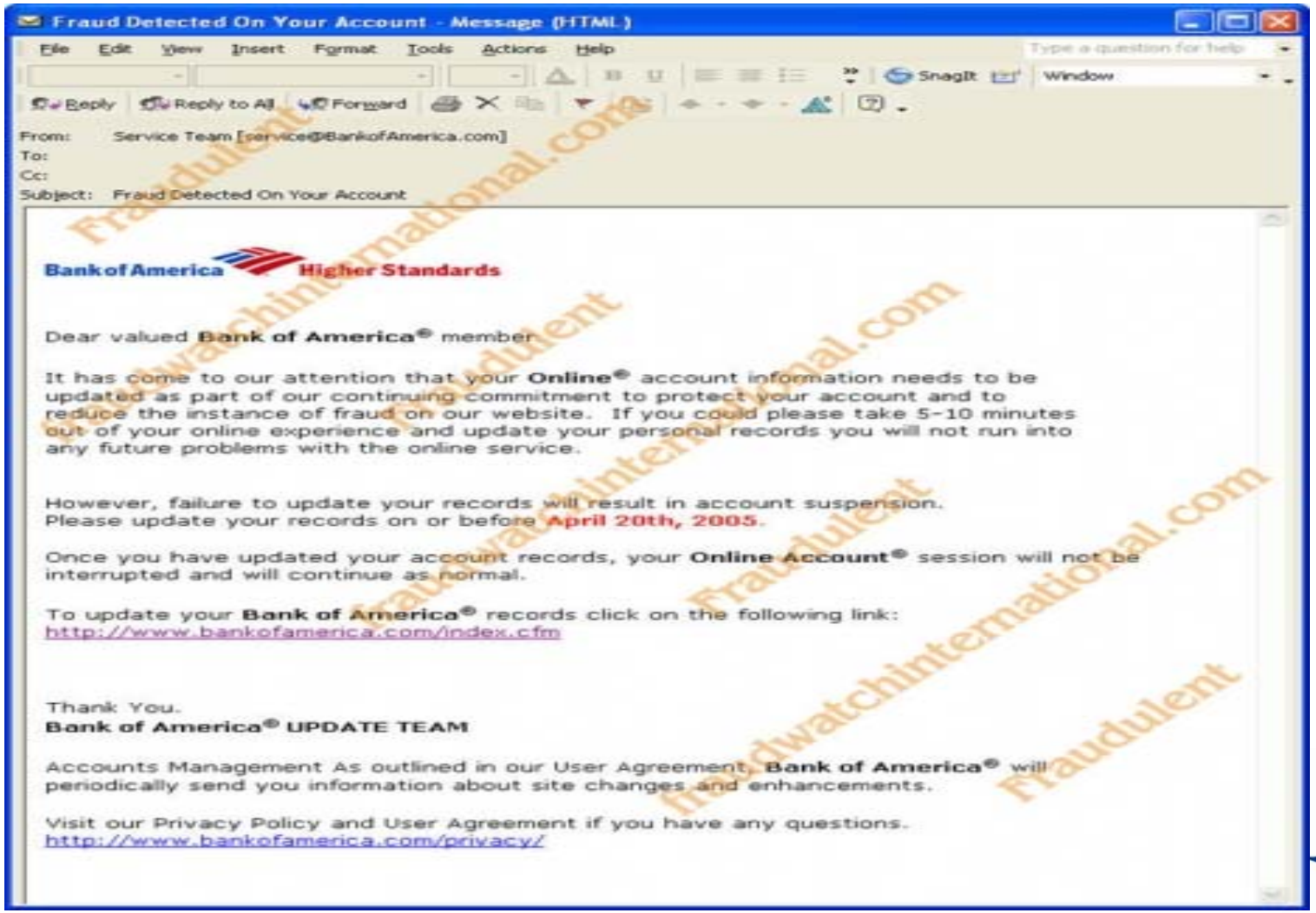
ICBA BANCARD &TCM BANK

DNS-Based Phishing (Pharming)

- DNS (Domain Name Server)-Based phishing refers to generally any form of phishing that interferes with the integrity of the lookup process for a domain name or website
- In January of 2005, someone fraudulently changed the DNS address for the domain Panix.com, a New York State Internet service provider. Ownership of the company was changed from New York to Australia. Requests to reach the Panix.com server were redirected to the United Kingdom, and e-mail was redirected to Canada. State and federal authorities are currently investigating this case.

ICBA
BANCARD
&TCM BANK

Phishing Email



Fraud Detected On Your Account - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: Service Team [service@BankofAmerica.com]
To:
Cc:
Subject: Fraud Detected On Your Account

Bank of America Higher Standards

Dear valued **Bank of America®** member

It has come to our attention that your **Online®** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.
Please update your records on or before **April 20th, 2005.**

Once you have updated your account records, your **Online Account®** session will not be interrupted and will continue as normal.

To update your **Bank of America®** records click on the following link:
http://www.bankofamerica.com/index.cfm

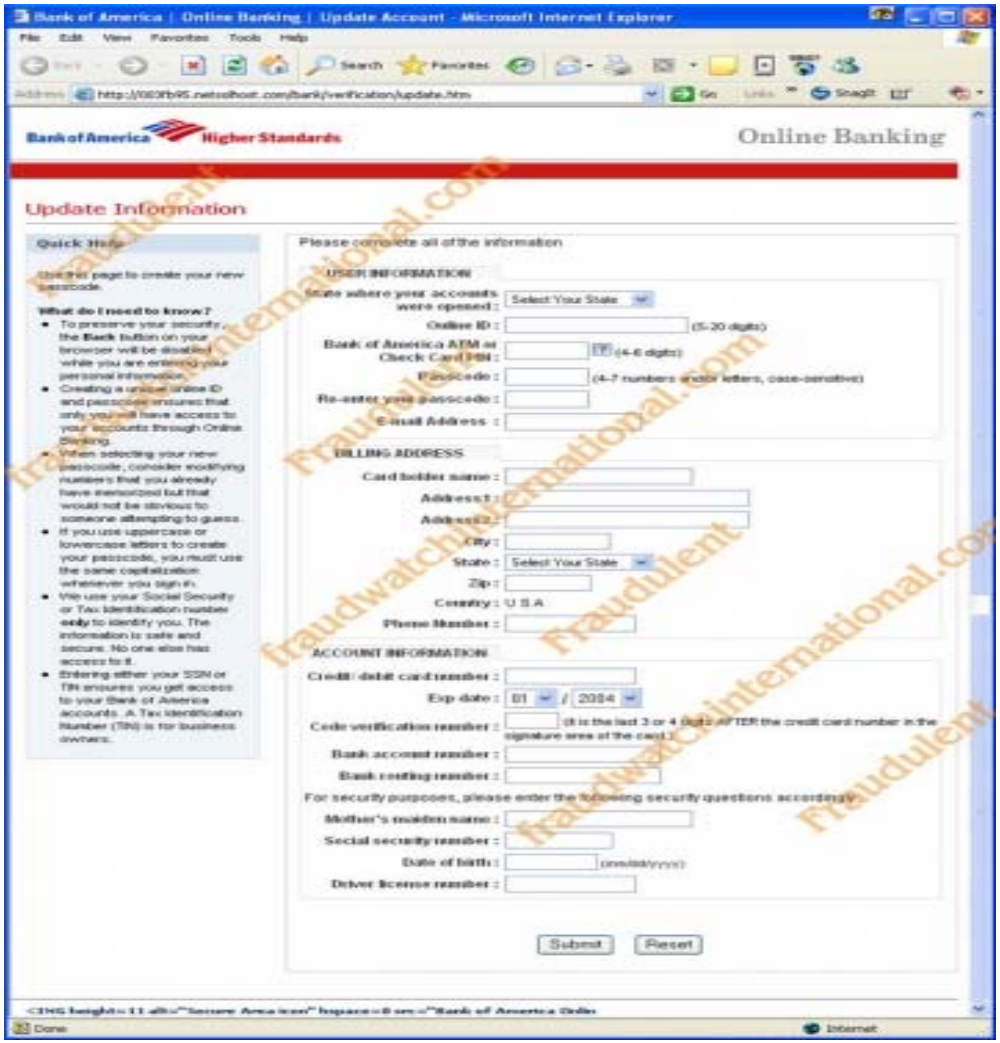
Thank You.
Bank of America® UPDATE TEAM

Accounts Management As outlined in our User Agreement, **Bank of America®** will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.
http://www.bankofamerica.com/privacy/

ICBA BANCARD &TCM BANK

Phishing Email



Phishing Prevention

- ***Web site protection***
  - ✓ Check your site often
  - ✓ Look for unauthorized links
  - ✓ Implement good quality anti-virus, content filtering, and anti-spam solutions
- ***Monitoring Services***
  - ✓ Name Protect, Mark Monitor, etc.
- ***Consumer Education***
  - ✓ Consumer knowledge is the most important prevention mechanism to stop fraud losses from Phishing

ICBA BANCARD &TCM BANK

Phishing Prevention

- Register the most deceptive available domain names similar to your brand. This is the cheapest insurance you can buy.
- Trademark your domain names to provide recourse against a party who registers deceptively similar domain names.
- Establish clear policies on your email practices, such as never asking for personal information or possibly never providing a clickable link in an email.
- Communicate your policies to your customers regularly, preferably in every email communication and in other media, such as printed statements.

ICBA BANCARD &TCM BANK

Phishing Prevention

- Provide an email address such as spoof@yourcompany.com, which customers may submit an email to and determine whether the email is legitimately from you or not.
- Provide clear instructions on your website, and in communications from your company, on how to report a phishing message.
- Establish a cross-functional task force responsible for responding to phishing attacks.

ICBA BANCARD &TCM BANK

Phishing Prevention

- Proactively prepare customer communications to be sent out in the event of a phishing attack.
- Monitor signs of a phishing attack, including email bounce messages, customer call volumes, anomalous account activity.
- Notify law enforcement promptly when a phishing attack is confirmed.
- When a phishing attack is confirmed, post an alert on your website and consider informing the customers of the attack via email.
- Trace the phishing servers and get them shut down as quickly as possible. (Service providers are available that can assist in this effort)

ICBA BANCARD &TCM BANK

Phishing Prevention

- Anti-phishing toolbars are promising tools for identifying phishing sites and heightening security when a potential phishing site is detected.
- Staff up your customer service when a large-scale phishing attack is confirmed.
- Preserve evidence of the phishing attack for subsequent prosecution of the phishers.

ICBA BANCARD &TCM BANK

Phishing Education

- www.antiphishing.org
- www.ic3.gov
- www.ftc.gov
- www.bbb.org/phishing
- www.mailfrontier.com
- http://usa.visa.com/personal/security/protect_yourself/common_frauds/phishing.html

ICBA BANCARD &TCM BANK

Voice Phishing - "Vishing"

ICBA
BANCARD
&TCM BANK

Voice Phishing - “Vishing”

Vishing:

(Voice Phishing) also called “Vishing”, is the voice counterpart to phishing. Instead of being directed by email to a web site, the user is asked to make a telephone call. The call triggers a voice response system that asks for the user’s credit card number.

ICBA BANCARD &TCM BANK

Voice Phishing - “Vishing”

- First Method: “Email Blast”
  - Related to phishing scams
  - Instead of a Weblink, perpetrators use phone numbers

Vishing - Example

PayPal®

Account Verification

Dear [redacted],
You have received this email because we have strong reason to belive that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

Voice Phishing - “Vishing”

- Second Method: “Cold-call Vishing”
  - War Dialer
    - An automated dialing program that relentlessly dials a large number of telephone numbers in the hope of finding anything interesting.
      - Voice Mail Boxes (VMB’s)
      - Private Branch Exchanges (PBX’s)
      - Computer modems (Dial-up)
  - VoIP (Voice over Internet Protocol)
    - Is a technology that allows anyone to make voice calls using a broadband internet connection instead of a regular phone line.

ICBA BANCARD &TCM BANK

Vishing – War Dialer Example

wdial200

Auto

```
                    WildDialer Version 2.0


                Number Dialed: 619-573-1257
                Modem Status : Dialing

                Number of Carriers: 0

                Search started at: 20:16:02
                Last call at     : 20:16:20


        Hit 'A' to abort search, >space< to cycle to next number.

 Area Code    : 619          Pulse/Dial: Tone          Wild Dialer V2.00
 Start Number: 573-1000      Delay: 20 seconds
 End Number   : 573-2000                               (C)opyright 1988
 Saving to: NUMBERS.TXT      Port: COM2                  by Pica Man
```

Report Vishing

- Internet Crime Complaint Center
  - http://www.ic3.gov
- Federal Trade Commission
  - http://www.ftc.org
- Directly to the company victimized by the scam

ICBA BANCARD &TCM BANK

Vishing - Prevention

- Tips to avoid vishing scams:
  - Avoid calling the number provided in the “vishing” email.
  - If you receive a “vishing” phone call, hang up.
  - Do not automatically trust a phone based on it’s area code.

ICBA BANCARD &TCM BANK

Counterfeit/
Counterfeit Skimming Fraud

ICBA
BANCARD
&TCM BANK

Counterfeit Fraud

- Criminals produce counterfeit cards by:
  - Manufacturing a card with the same appearance of a valid card
  - Re-embossing or re-encoding from a once legitimate lost/stolen/NRI card
  - Re-embossing or re-encoding from a fraudulently manufactured card (skimming)

ICBA BANCARD &TCM BANK

Counterfeit Skimming

- Replication of the magnetic stripe data on a credit or debit card
- Initial fraud occurs at a merchant location during a valid transaction
- Account number, expiration date, CVV/CVC obtained
- Reads through the system as POS 90 or card present transactions
- Target businesses
  - Gas stations
  - Hotels
  - Restaurants

ICBA BANCARD &TCM BANK

Counterfeit Skimming

Most skimming operations consist of many criminal elements working together forming sophisticated crime rings with specific roles

- Skimmers – frontline recruit -persons actually stealing the information at a business
- Runners – persons using the magnetic strip data or counterfeit cards to make purchases or cash advances
- Middlemen – organizes the operation and distributes the cards to runners

ICBA BANCARD &TCM BANK

Counterfeit Skimming Needs

- Materials (hardware and software) used in scheme execution
  - Skimming instruments (readers, wedges, skimmers)
  - Personal and laptop computers
  - Cables and hookups
  - Plastic cards
  - Card encoding software programs

ICBA BANCARD &TCM BANK

Skimming Starter Kit

ICBA BANCARD &TCM BANK

Handheld Skimming Device

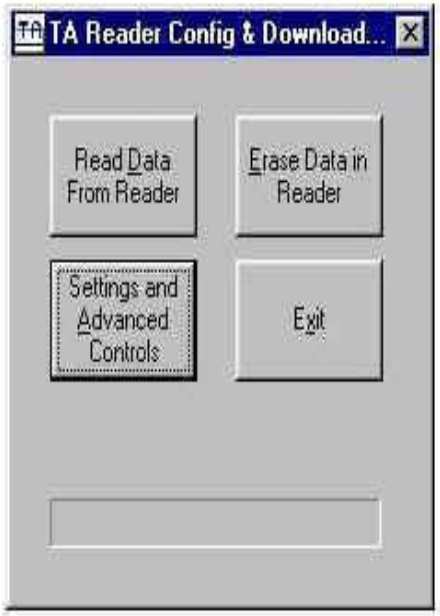
ICBA
BANCARD
&TCM BANK

Skimming Computer Setup

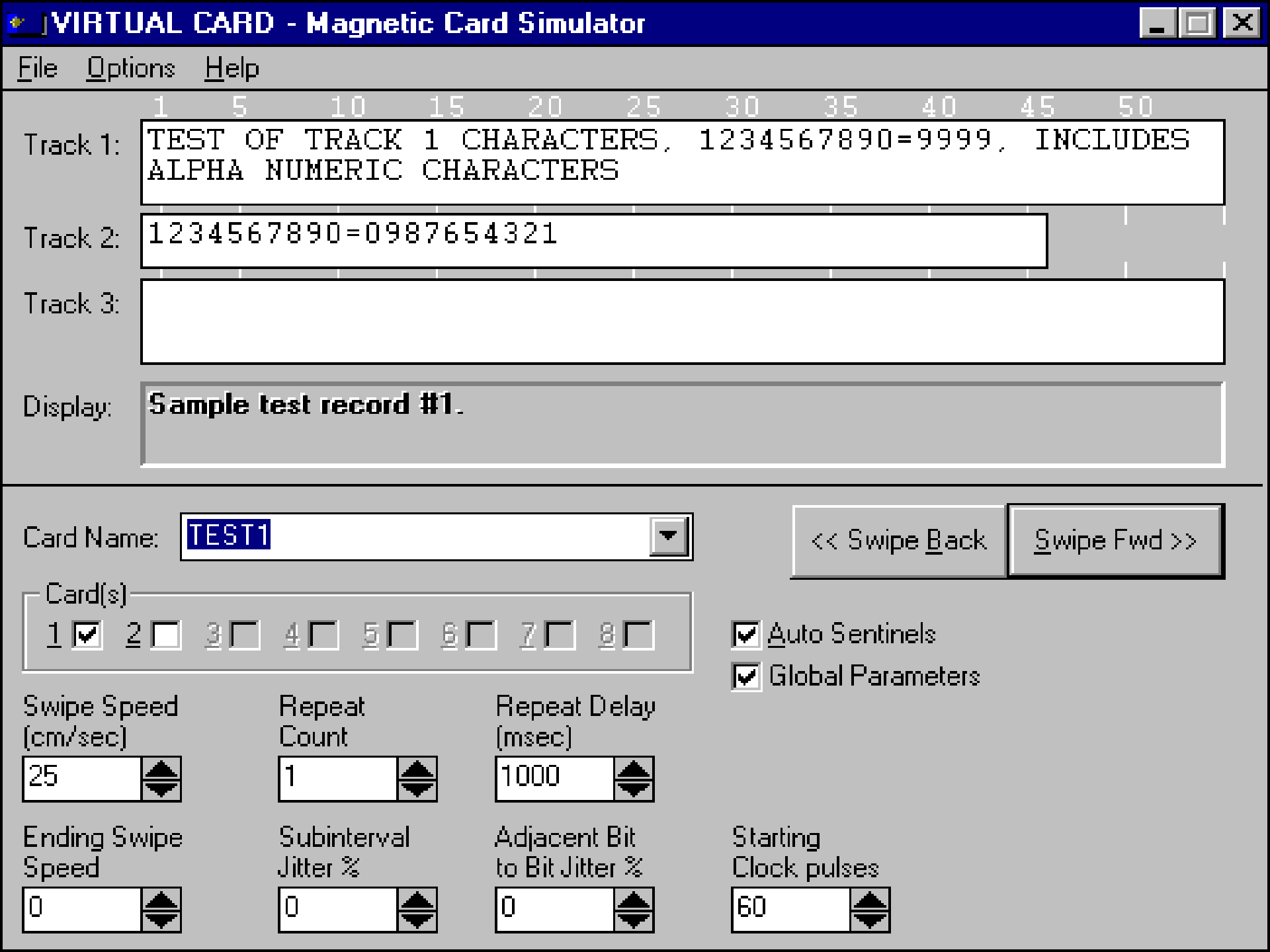
Alternative Skimming Devices

ICBA
BANCARD
&TCM BANK

Skimming



JCBA
BANCARD
&TCM BANK


VIRTUAL CARD - Magnetic Card Simulator
File Options Help
1 5 10 15 20 25 30 35 40 45 50
Track 1:
TEST OF TRACK 1 CHARACTERS, 1234567890=9999, INCLUDES ALPHA NUMERIC CHARACTERS
Track 2:
1234567890=0987654321
Track 3:
Display:
Sample test record #1.
Card Name:
TEST1
<< Swipe Back
Swipe Fwd >>
Card(s)
1 2 3 4 5 6 7 8
Auto Sentinels
Global Parameters
Swipe Speed (cm/sec)
25
Repeat Count
1
Repeat Delay (msec)
1000
Ending Swipe Speed
0
Subinterval Jitter %
0
Adjacent Bit to Bit Jitter %
0
Starting Clock pulses
60

Skimming Equipment

- Skimming Door Devices

ICBA BANCARD &TCM BANK

Handheld Skimming Devices

ICBA
BANCARD
&TCM BANK

Skimmer & Palm Pilot

ICBA BANCARD &TCM BANK

ATM Skimming

ATM SKIMMING AND PIN COMPROMISE

In Security Alert AP1/04 issued 13 January 2004, MasterCard International informed you about several cases of alleged card data and PIN compromise at automatic teller machines (ATM's) in Australia, Taiwan and Hong Kong within the Asia / Pacific Region.

Further instances of this activity have recently occurred in Melbourne, Australia.

Primary Equipment Involved

- ***Skimming Device*** to capture and store card track information of unsuspecting cardholder as the card is inserted into the card reader slot of ATM (see figure 1 below)

ICBA BANCARD &TCM BANK

ATM Skimming

Modus Operandi

- **Skimming device** inserted into the card reader slot to capture and store card track data as the ATM processes the cardholder transaction.
- **Fake ATM pin-pad** placed over the genuine pin-pad to capture and store key strokes as the cardholder enters their PIN.
- The recently recovered **skimming devices** bear strong similarities to devices recovered in Europe, the Middle East and more recently in London. The one major difference between the Australian devices and the others is the Australian devices were storing card track data. The European and Middle East devices were transmitting the stolen card track data.

Signs of ATM Tampering

- ATM's retaining white plastics – an indication of ATM testing.
- Remnants of glue or stickers on the ATM.
- Unidentified objects attached to the ATM.

ICBA BANCARD &TCM BANK

ATM Skimmer – Card Reader

Primary Equipment Involved

- *Skimming Device* to capture and store card track information of unsuspecting cardholder as the card is inserted into the card reader slot of ATM (see figure 1 below).

Figure 1 – Fake ATM card slot with microchip to store track data.

ATM SKIMMER –PIN Reader

Fake ATM pin-pad overlaid onto ATM pin-pad to capture and store the Pin as it is entered by the cardholder (see figure 2 below).

Figure 2 – fake ATM pin-pad recovered following similar event in Taiwan. The pin-pads used in the recent Australian attacks have not been recovered but cardholders did report difficulty in entering their PIN as well as the pin-pad appearing to have an additional layer over it.

ATM Skimmer

This ATM skimmer device, which was attached to a Bank of America ATM in Boca Raton, Fla., shows the touch-screen in the center with the card swipe on the right-hand side.

Photo provided by: Palm

http://www.bankrate.com/brm/news/atm/20021004a.asp

ATM Skimming Device

ICBA
BANCARD
&TCM BANK

Counterfeit Skimming Prevention

- New technology
  - Chip cards
  - Biometrics
  - Imaging
- Neural networks (Falcon)
- Report monitoring - Focus on valid POS 90 transactions on accounts with fraudulent POS 90 transactions
- Report activity to Visa and MasterCard
  - (if CPP is identified)

ICBA BANCARD &TCM BANK

Data Compromises

ICBA
BANCARD
&TCM BANK

Evolution of Data Compromises

eCommerce ⇒ Retail ⇒ Processors ⇒ PINs

- eCommerce – account number
- Retail – magnetic stripe data
- Processors and Third Party Vendors – track data & large numbers of accounts
- Capture of track data, PIN blocks, encryption keys

ICBA BANCARD &TCM BANK

Data Compromises

- Shift of hacker focus from ecommerce to retail merchants
- Increase in track data compromises as well growth of PIN compromises is increasing
- Incidents involving stolen laptops and/or data tapes is on the rise
- Effect of data compromises help explain the rise in overall fraud rates and dollar losses in counterfeit as well account takeovers

ICBA BANCARD &TCM BANK

Data Compromise Trends

- Data Recovery
  - Law Enforcement
  - Online Chat Rooms
- Lost or Stolen Data
  - Missing back-up tapes
  - Stolen hard drives
- Network Intrusions
  - Physical hacks
  - Uninvited network incursions/sniffing

ICBA BANCARD &TCM BANK

Current Compromise Targets

- Small merchants in service industries
  - Vulnerable POS applications
  - Open wireless access points
  - No intrusion detection or firewalls
  - Non existent logging
- National retailers with a centralized corporate network
  - Unpatched operating systems
  - Default configuration for many applications
  - Minimal network segmentation allows full access
    - Once they get into the network, they can go anywhere

ICBA BANCARD &TCM BANK

Data Compromises

- Many retail systems use standard passwords for data storage & remote technical support
- Smaller merchants have fewer resources to focus on security
  - Some inadvertently store track data
  - Weak passwords, not frequently changed
- High staff turnover increases likelihood of passwords becoming known

ICBA BANCARD &TCM BANK

San Francisco Chronicle

Personnel shake-up at VA over data theft Analyst whose PC was stolen to be fired -- 2 bosses also out

Christopher Lee, Washington Post
Wednesday, May 31, 2006

* Printable Version
* Email This Article

Washington -- Secretary of Veterans Affairs Jim Nicholson announced several personnel changes Tuesday that will include the firing of a senior career **data** analyst who lost the sensitive personal information of millions of veterans.

The 60-year-old civil servant, who earns $91,407 to $118,828 a year, has been notified he will be terminated, **VA** officials said. The employee violated department policy by taking home electronic files containing the names, birth dates and Social Security numbers of as many as 26.5 million veterans.

IRS Laptop Lost With Data on 291 People

By Christopher Lee
Washington Post Staff Writer
Thursday, June 8, 2006; Page A04

An Internal Revenue Service employee lost an agency laptop early last month that contained sensitive personal information on 291 workers and job applicants, a spokesman said yesterday.

The IRS's Terry L. Lemons said the employee checked the laptop as luggage aboard a commercial flight while traveling to a job fair and never saw it again. The computer contained unencrypted names, birth dates, Social Security numbers and fingerprints of the employees and applicants Lemons said. Slightly more than 100 of the people affected were IRS employees, he said. No tax return information was in the laptop, he said.

Digital Crime Wave - The Growing Problem

CTR, CA - Jun 1, 2006
... **Intrusion** cost the United States $17.5B in 2004. ...

abc 7NEWS
THEDENVERCHANNEL.COM

SEARCH
Powered by YAHOO! SEARCH
SITE WEB
YELLOWPAGES.COM

Local News
The Investigators
News Tips
Weekly Archive
Most Popular
Weird Headlines
7 News Team
E-mail Alerts
Forums

NEWS
Home
Local News
National News

Homepage > News

Park At DIA? Your Credit Card Info Was Stolen

Airport Managers Knew About Theft 10 Days Ago

POSTED: 5:14 pm MST February 23, 2006
UPDATED: 5:12 am MST February 24, 2006

Email This Story | Print This Story

DENVER -- There's bad news for anyone's who's parked at Denver International Airport and used a credit card to pay in the last seven years. Your credit card information has been stolen.

Lost Digital Data Costs Businesses Billions

By Stephanie Armour

CONSUMER WATCH: Suits follow breaches of client data

IRIS TAYLOR
TIMES-DISPATCH COLUMNIST
May 28, 2006

It was bound to happen.

First, there was a rash of consumer privacy breaches that seemed to spiral after the high-profile data leak at ChoicePoint Inc. of Alpharetta, Ga., in 2005.

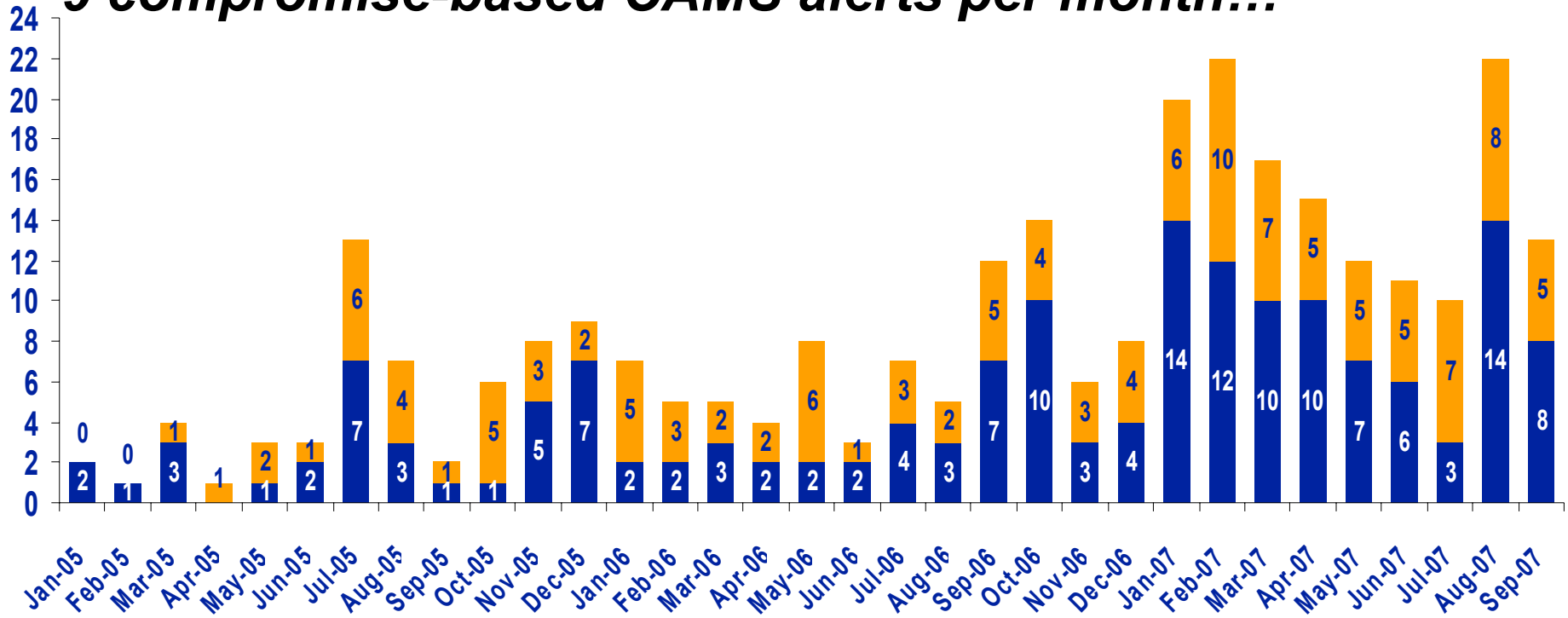
Now -- one year and hundreds of breaches later, including the latest theft of 26.5 million veterans' Social Security numbers -- lawsuits are pouring onto court dockets nationwide.

Privacy & American Business, an organization based in New Jersey that tracks consumer privacy lawsuits, is watching 22 cases nationwide, including 13 actions at the Federal Trade Commission, said Lyle Himmel, the group's staff attorney.

The latest action resulting in a settlement was against Nations Title Agency Inc. of Kansas City, Kan., on May 10. The FTC also is conducting other investigations, staff member Alain Sheer said.

Hacking Incidents - By type

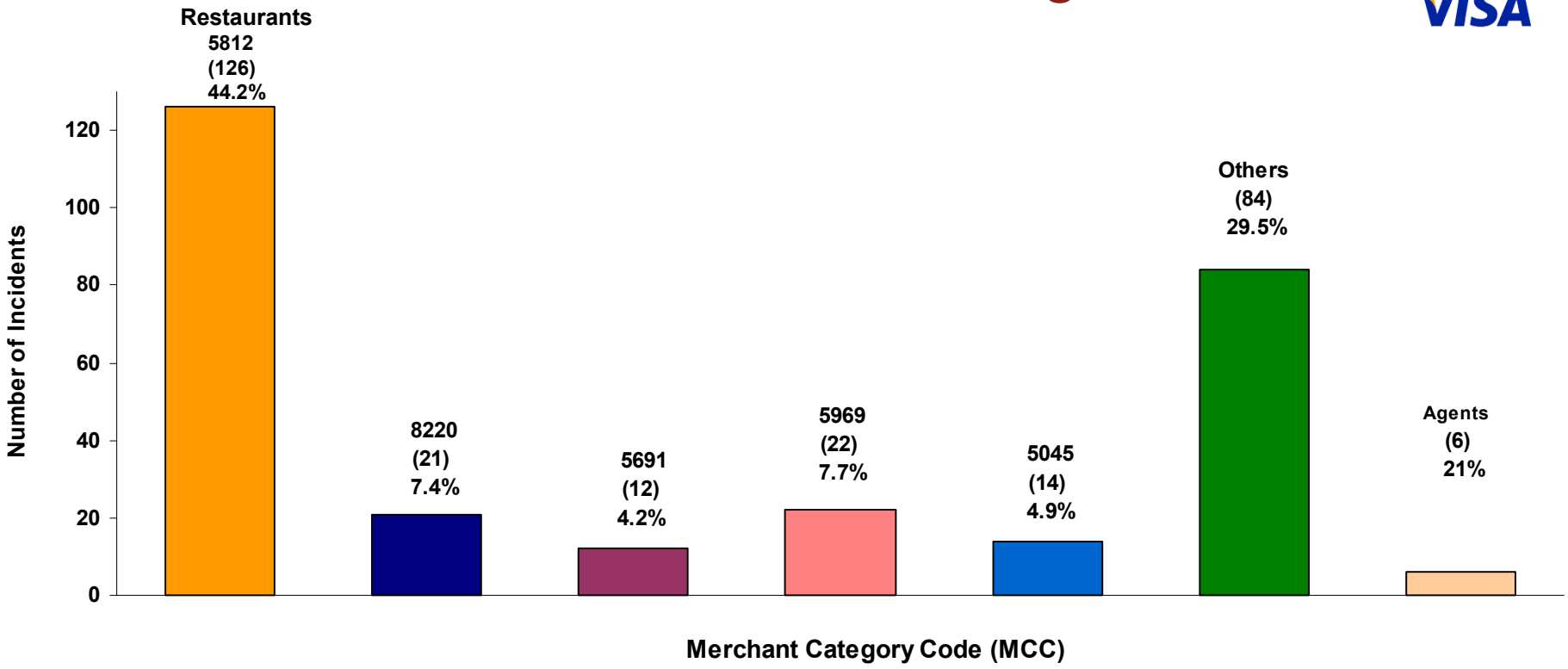
Since January 2005, Visa has distributed an average of 9 compromise-based CAMS alerts per month…



* Date reported is based on CAMS alert date

Hacking Incidents - by MCC January 2005 to September 2007

Food service entities targeted…

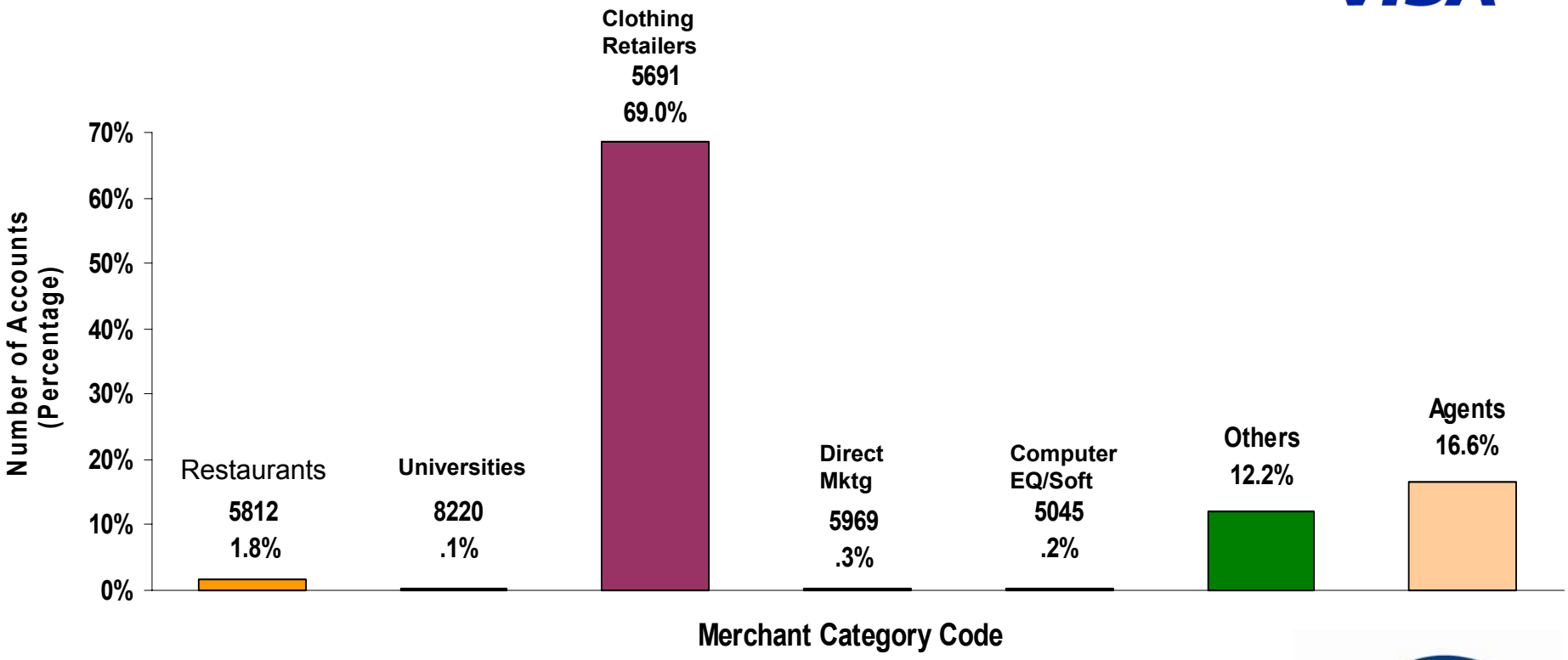


Total Number of Compromise Incidents (Hacks) = 285

* Agents = ISOs, Processors, Third Party Processors, etc.

Hacking Incidents (Compromised Accounts by MCC) Jan 2005 to September 2007

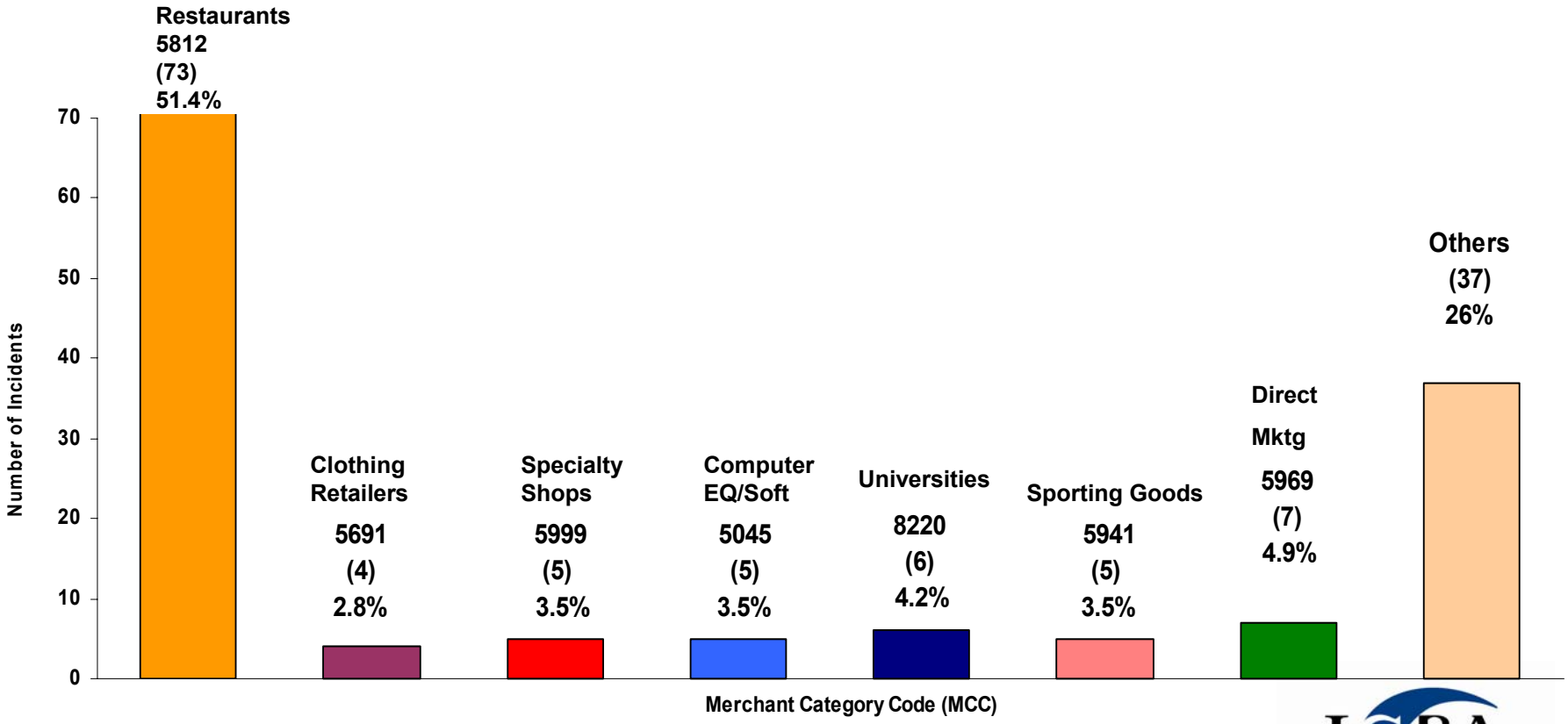
But large retailers and agents present greatest exposure



* Agents = ISOs, Processors, Third Party Processors, etc.

Hacking Incidents by MCC Year to date – September 2007

Total Number of Compromise Incidents = 142



* Agents - ISOs, Processors,Third Party Processors, etc..

“Carder” Trends

- 86% of cards for sale on underground are issued by banks in the United States*
- Financial services sector account for 84% of the brands phished in 2006*
- Online, fully automated ordering systems for stolen card data available 24/7
  - Inventories of as many as 800,000 stolen cards per site
  - Tiered pricing available
  - Pre-purchase testing validation available
- Current market value

* Source: Symar
(1st volume to feature the “Underground Economy Servers” category)

Organizational structure and data flow

- **Organized crime follows a business-like structure and separates duties**

Recon/Hackers
- Looks for zero day exploits
- Wide range scanning, looking for systems/POS/databases that are vulnerable
- Scanning/probing for specific targets
- Steals account information

Data Cleansers/ Aggregators
- Responsible for data preparation
- Sorts by BIN, product, country etc.
- Tests data for authorizations, limits, weak authorization parameters

Sellers
- Vets potential buyers
- Arranges payments

Crackers
- Takes leftovers from cleansers
- Breaks encrypted data
- Tries to crack encryption, PIN blocks

Customers/ Resellers
- Purchases data or plastic
- Creates counterfeit cards
- Performs fraudulent purchases
- Resells data or plastic

ICBA BANCARD &TCM BANK

Carder Sites

"I sell the freshest DUMPS, they are mostly USA, some EU and Asia."

"You can choose your favorite BIN's from over 300K or I will do it myself."

Prices: USA Visa or MC gold/platinum: $25

Payment: Egold: minimum $100

ICBA BANCARD &TCM BANK

Edit View Favorites Tools Help

Favorites

http://cardingworld.cc/

Go

КАЧЕСТВЕННЫЙ

Форма заявки Search Members Calendar

menu has been disabled

Глобальный поиск по статусу, имени, icq, e-mail

Все пользователи

ok!

Умные люди здесь делают бабки!!!

VISA classic $8 | EU ASIA

Just Buy It

SE-CODE

Firefox Module - http, https, java & flash keys grabber

по поводу размещения рекламы обращайтесь David® icq: 443036

www.CardingWorld.cc

Board Message

e error returned was:

u do not have permission to view this board

u are not logged in, you may log in below

Only messages related to **current** events.

Cvv2 From Garza! (visa/mc/amex/disc). All Countrys, All Banks! Good Price!

Posted by: **Garza** (---.fastres.net)
Date: January 10, 2007 04:29AM

Hello people!
I'm Garza, verified cvv2 seller on Mazafaka, DM, CardingWorld.

I'm providing a fresh cards (cvv2, vbv) from first hands!
I'm not reseller!! Becouse my price is too low.

My price is:

USA
1 approved card + Cvv2 = 1$!!! (>100cc's)
100cvv2 - 100$
1000cvv2 - 700$

1.5$ per 1 approved cvv2 <100 cc's.

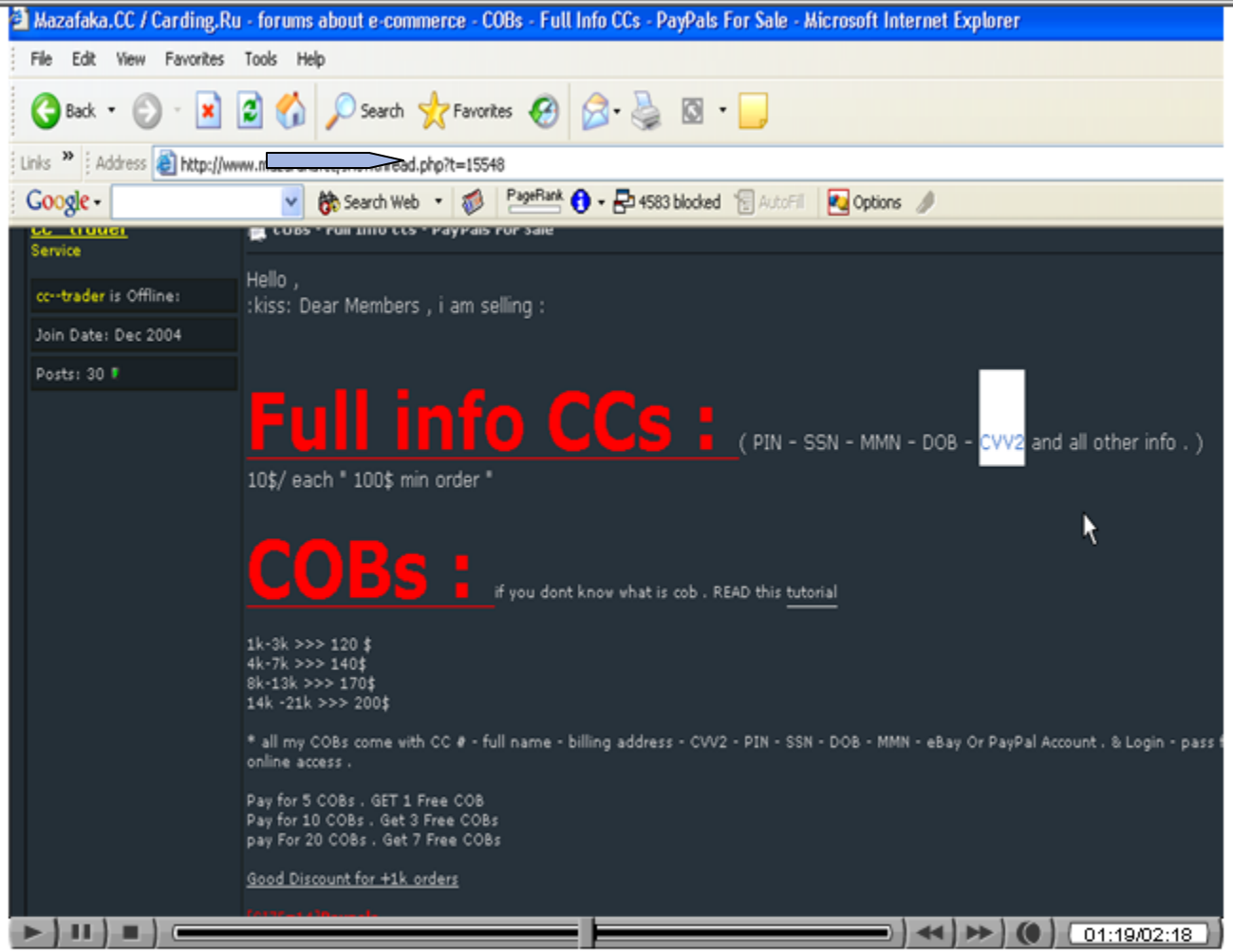
EU (75 countrys available!)
1 approved cvv2 card + Cvv2 = 2$!!!
1000cvv2 - 900$
Countrys available now: US,AU,CA,NZ,NL,ES,IT,JP,KR,FR,DE,DK,SE,SK,BE,PL,IE ,IO,UK,AO.AE,NO,MX,ZA and others!!

Edit View Favorites Tools Help

Favorites

http://www.identitytheftsecrets.com/videos/mazafaka.html

Go



Comment on this video in our forum Комментарии - форум

CAN'T SEE THE VIDEO? Download Shockwave.

Get Adobe Shockwave Player

Get Shockwave

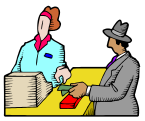
Sophisticated Supply Chain

CONSUMERS

Stores

Financial Institutions

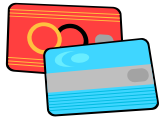
Processors



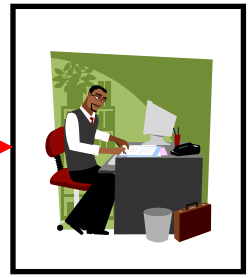
Restaurants

1. Consumers Conduct Business

2. Track Data Stolen



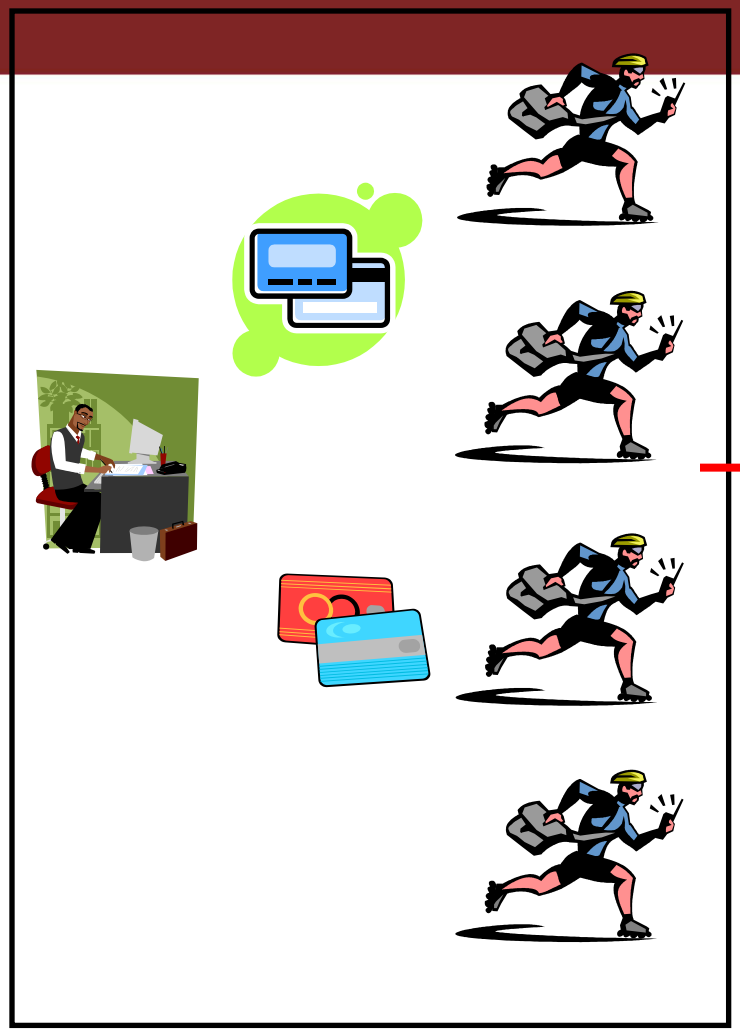
3. Cards need to be produced



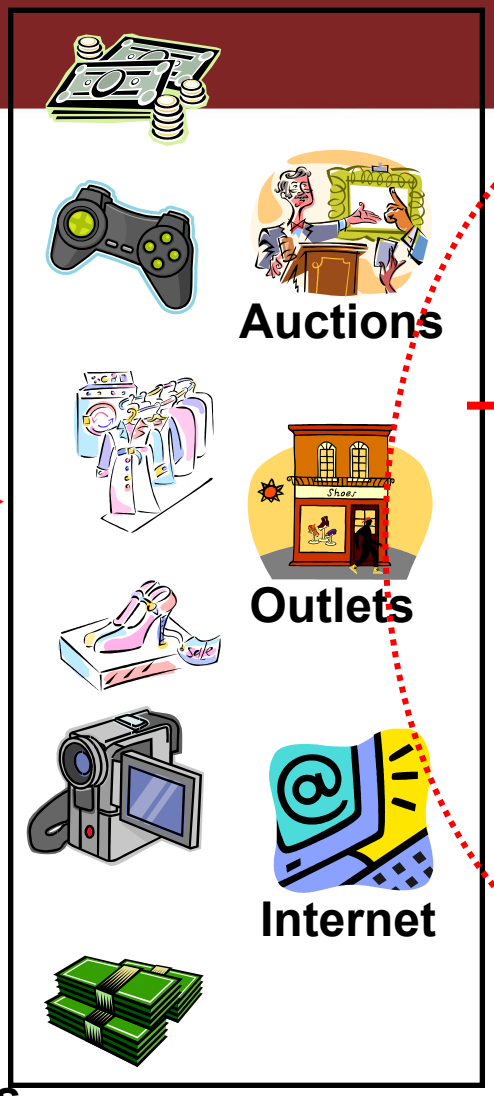
4. Broker found

ICBA BANCARD &TCM BANK

Sophisticated Supply Chain

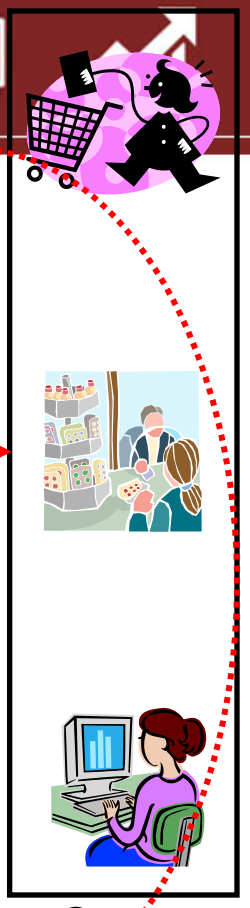


5. Broker distributes Cards



6. “Runners” buy and supply merchandise

RESHIPPERS



7. Consumers purchase goods

Visa CAMS and MasterCard Alerts

- Review alerts immediately
- Block and reissue when necessary
- Watch for fraud patterns
- Have a set procedure
- Archive all account lists and notices for several years
- Notify cardholders before blocking compromised accounts

ICBA BANCARD &TCM BANK

Account Compromise Prevention

- Secure merchant data sites
  - Visa and MasterCard mandates
- Neural Networks (Falcon)
- Report Monitoring
- CAMS and MasterCard Alert Management
  - Review all alerts
  - Take appropriate actions

ICBA BANCARD &TCM BANK

Identity Theft

ICBA
BANCARD
&TCM BANK

Identity Theft

- What is Identity Theft?
- Why does Identity Theft occur?
- Who are the perpetrators?
- Who are the victims?
- What can be done?

ICBA BANCARD &TCM BANK

Identity Theft

- Industry confusion
- Credit & Debit card issuers
- Consumer actions
- Impact of internet and computers
- Criminal motivation

ICBA
BANCARD
&TCM BANK

Identity Theft Defined

- The Identity Theft and Assumption Deterrence Act of 1998 –

- Federal Government View
  - The ID Theft act amends 18 U.S.C. 1028 to prohibit: knowingly transfer[ing], without lawful authority, a means of identification of another person with the intent to commit, aid, or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.

ICBA BANCARD &TCM BANK

Identity Theft Re-defined

- The Visa ID Theft working group definition:
  - "Identity Theft involves manipulating or improperly accessing another person's identifying information, such as social security number, mother's maiden name, or personal identification number (rather than account number) in order to fraudulently establish credit or take over a deposit, credit or other financial account for benefit. Identity theft compromises a consumer, rather that an account or multiple accounts."

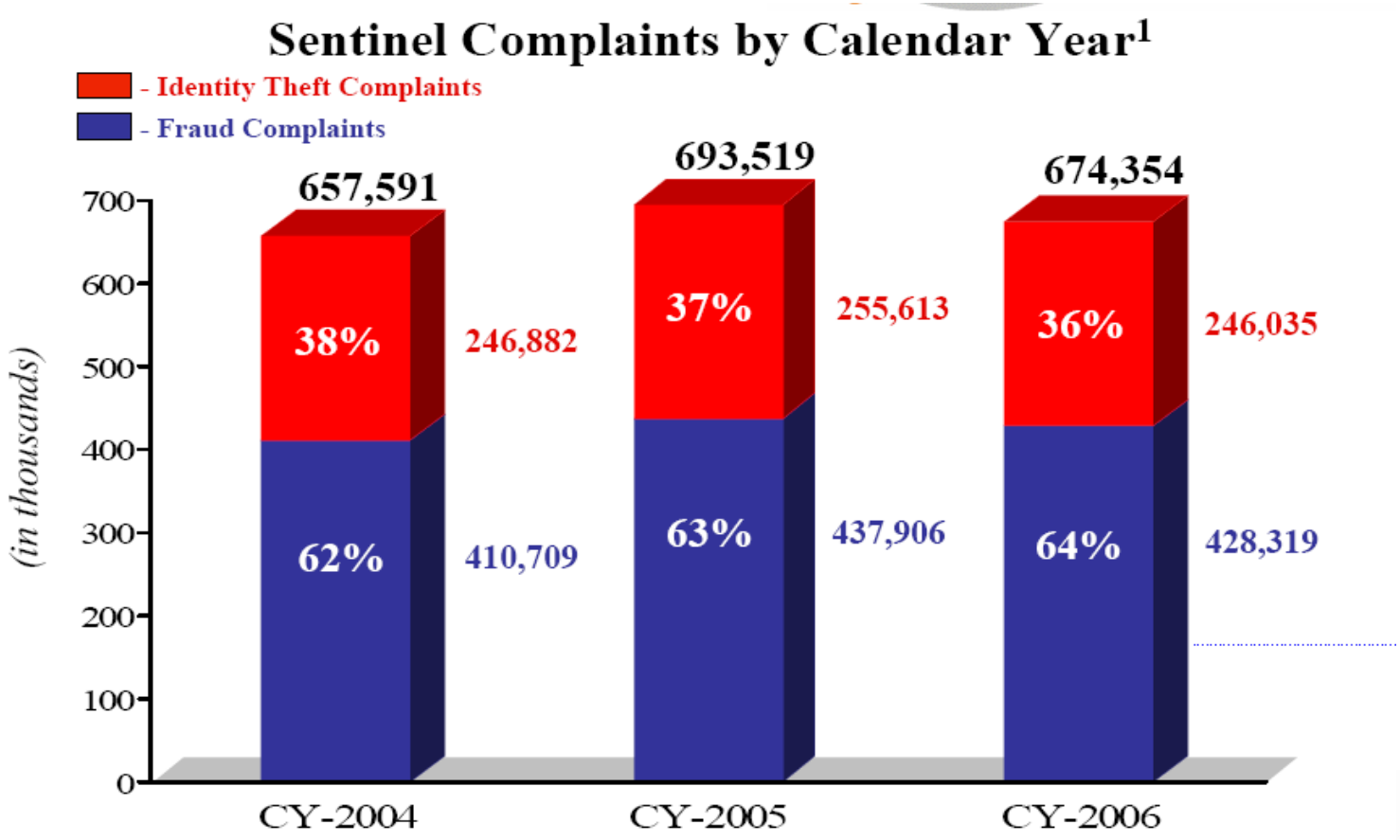
ICBA BANCARD &TCM BANK

Importance of Understanding IDT

- Understanding IDT allows staff to…
  - Better distinguish and handle cases
  - Detect IDT scams
  - Set policies and procedures
  - Assist victims
  - Assist law enforcement officials
  - Accurately report incidents

ICBA BANCARD &TCM BANK

Consumer Sentinel Fraud Complaints



[1]Percentages are based on the total number of Sentinel complaints by calendar year. These figures exclude National Do Not Call Registry complaints.

ICBA BANCARD &TCM BANK

Costs of ID Theft - Card Issuers

- Institutions absorb much of the economic costs of IDT…
  - Fraud transactions
  - Blocking accounts
  - Reissuing accounts
  - Validating customers
  - Implementing prevention programs
- Unauthorized use of a card DOES NOT necessarily constitute IDT.

ICBA BANCARD &TCM BANK

Costs of ID Theft – Perceived

- Unfair legal rulings
- Lack of consumer confidence
- Community cost for expanded law enforcement services
- Unknown dollars flowing into organized criminal groups

ICBA BANCARD &TCM BANK

Identity Theft Perpetrators

- ID Theft perpetrators vary in the following characteristics:
  - Age
    - Tech savvy teens to reclusive adults
  - Educational level
    - College graduates to high school drop-outs
  - Motivation
    - Sophisticated fraud rings to petty drug addicts

ICBA BANCARD &TCM BANK

Identity Theft Victims

- Identity theft victims are of all races, incomes, and ages
- More than 33 million Americans (about 1 in 6 adults) claim to have had their identities used by someone else since 1990
- There were reported 9.9 million victims in the last year alone (4.6% of the population)
- Victims typically lose $800 and spend two years clearing up their names

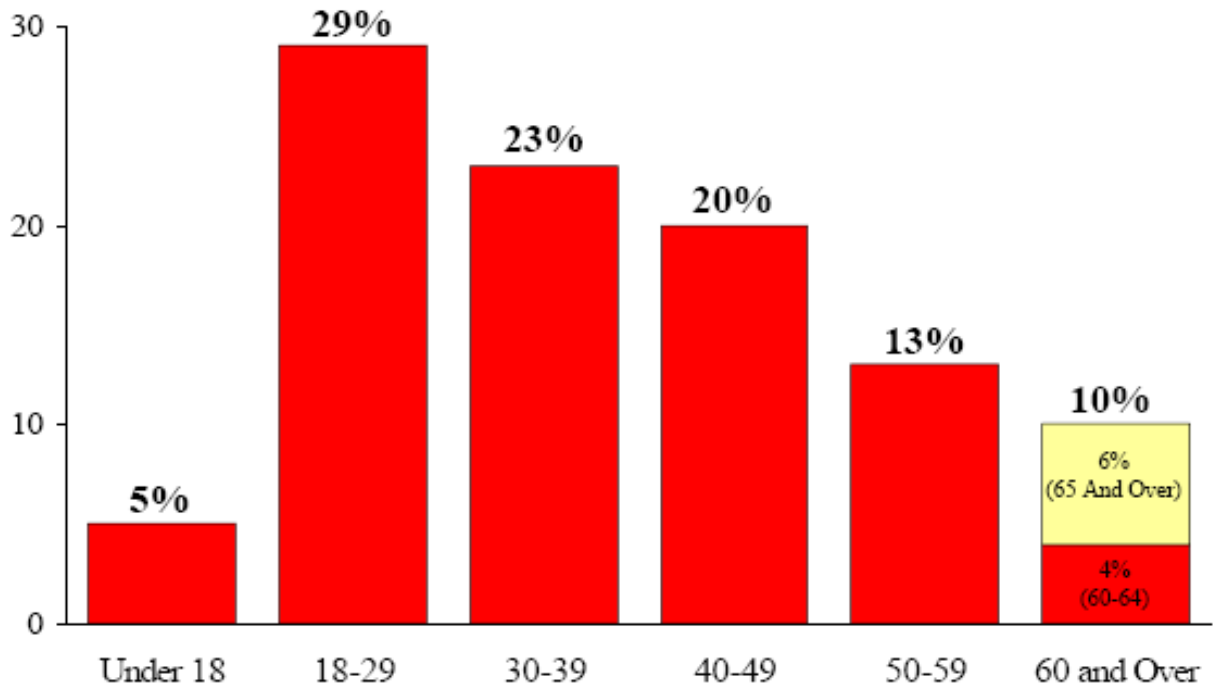
ICBA BANCARD &TCM BANK

Victim Characteristics

Identity Theft Complaints by Victim Age[1]

January 1 – December 31, 2006

IDENTITY THEFT Data Clearinghouse



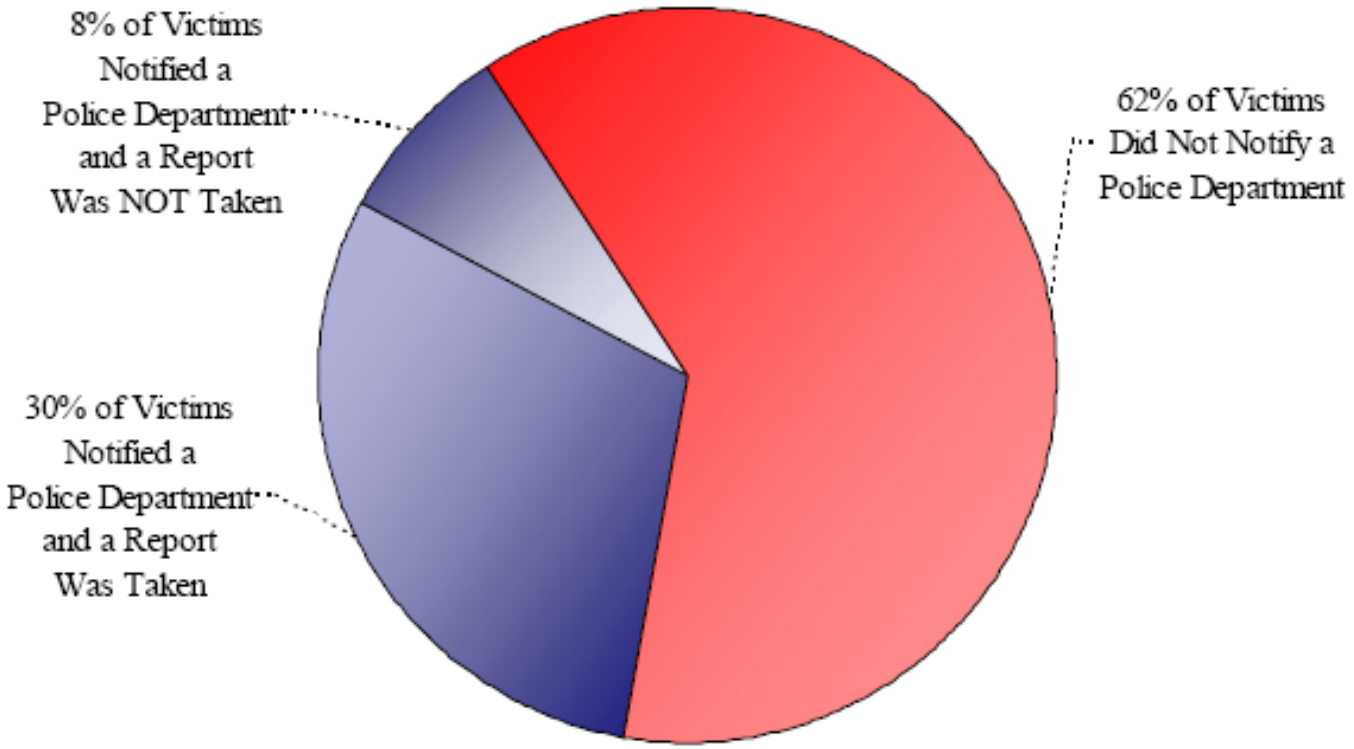
[1]Percentages are based on the total number of identity theft complaints where victims reported their age (225,532). 94% of the victims who contacted the FTC directly reported their age.

ICBA BANCARD &TCM BANK

Reporting Characteristics

Law Enforcement Contact[1]

January 1 – December 31, 2006

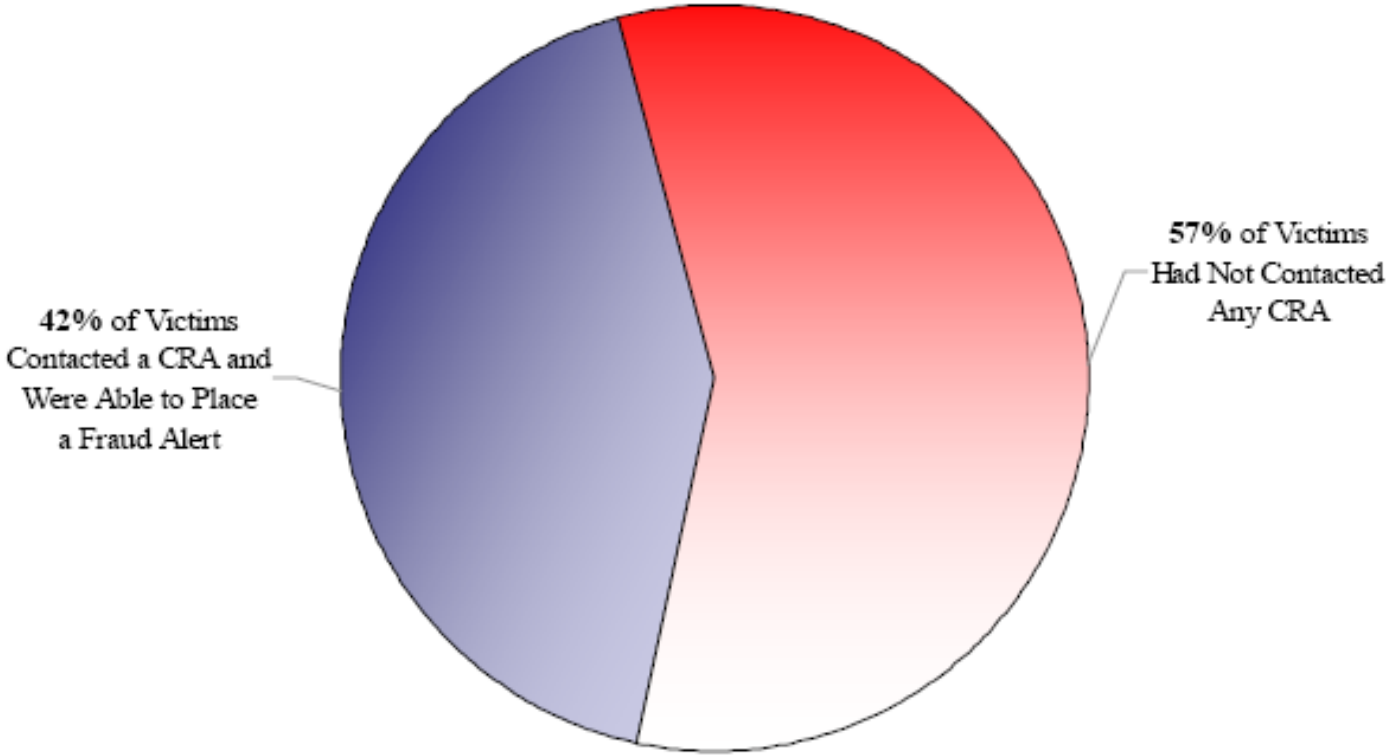


ICBA BANCARD &TCM BANK

Reporting Characteristics

Credit Reporting Agency (CRA) Contact[1]

January 1 – December 31, 2006



Source: Federal Trade Commission

Identity Theft – Top 10

Top 10 states for identity theft (on per-capita basis)

Rank	State	Victims/100,000
1	Arizona	147.8
2	Nevada	120
3	California	113.5
4	Texas	110.6
5	Florida	98.3
6	Colorado	92.5
7	Georgia	86.3
8	New York	85.2
9	Washington	83.4
10	New Mexico	82.9

Source: Consumer Sentinel

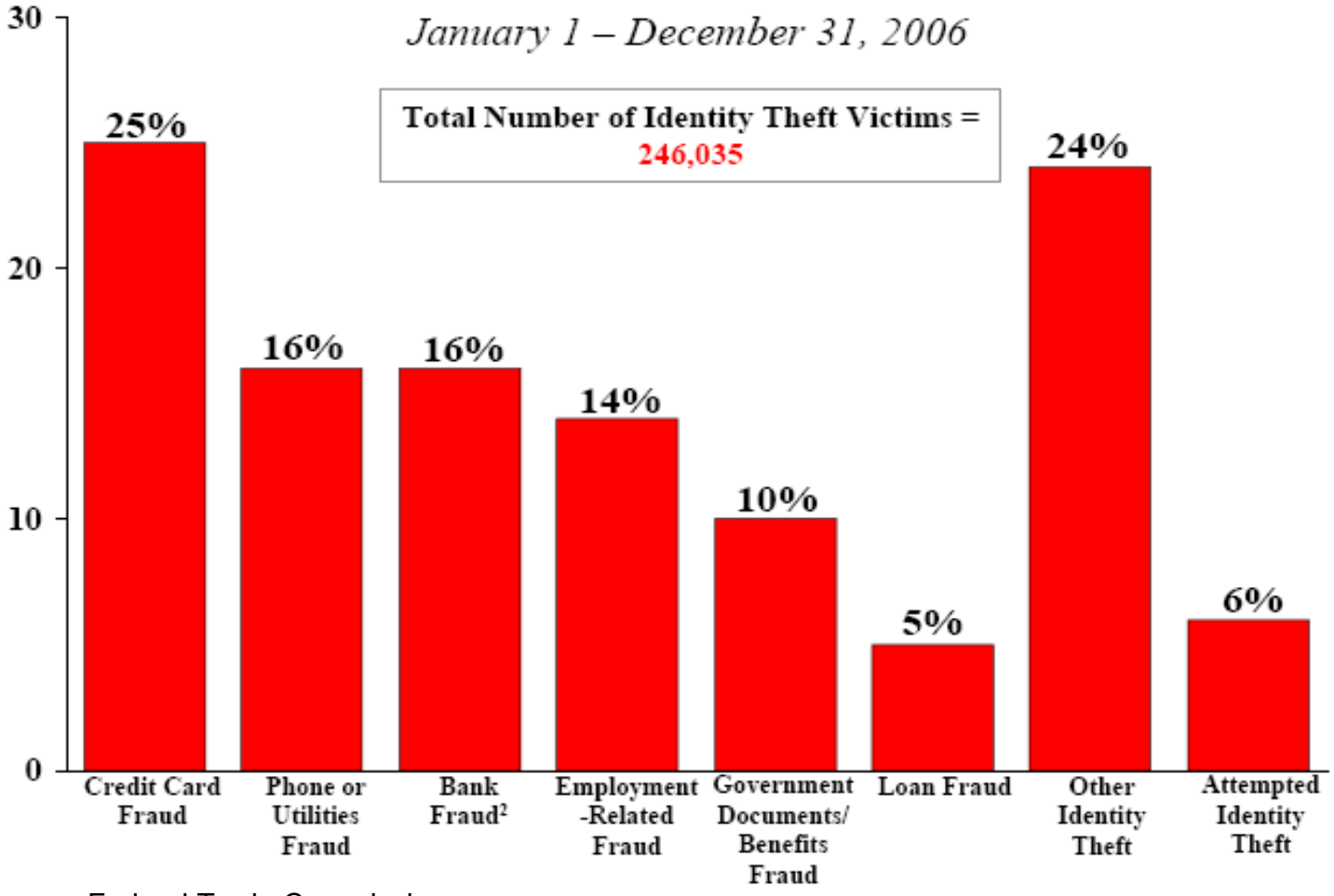
ICBA BANCARD &TCM BANK

Identity Theft Misused

How Victims' Information is Misused[1]

January 1 – December 31, 2006

Total Number of Identity Theft Victims = 246,035



Source: Federal Trade Commission

ICBA BANCARD &TCM BANK

Role to Assist IDT Victims

- Financial institutions are in the best position to assist IDT victims. Be sure to…
  - Train employees in detection and prevention
  - Have clearly written ID theft claims policies
  - Comprise fair investigation procedures
  - Have methods for follow-up and close cases
  - Assist law enforcement and legal contacts

ICBA BANCARD &TCM BANK

Identity Theft Prevention - Consumers

FI's should strongly encourage and promote…

- Usage of secured Websites
- Usage of encryption technology with all Website products and services
- Consistent cardholder education reinforcing the importance of safeguarding personal information
- Guidance in assisting customers and IDT victims
- The need to report all IDT cases to law enforcement

ICBA BANCARD &TCM BANK

Identity Theft Prevention - Issuers

- Research ALL listed addresses and telephone numbers of applicants
- Be aware of recently moved or out of state address changes
- Always request cardholder disputes and claims in writing
- Implement password change policies throughout the enitre organization

DETER·DETECT·DEFEND
AVOID THEFT

ICBA
BANCARD
&TCM BANK

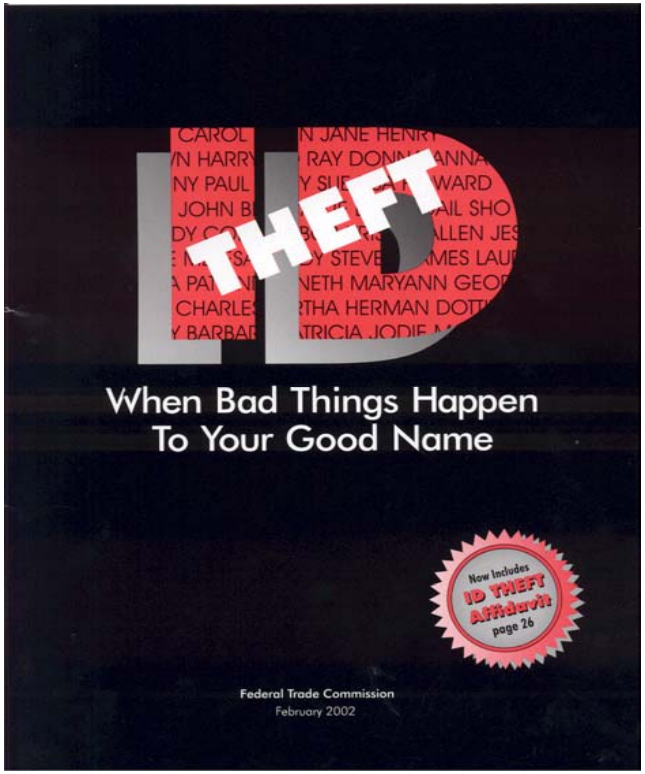
Credit Bureaus

- **Equifax Credit Information**
  - Telephone Number: (800) 997-2493
  - Fraud Line: (800) 525-6285
  - Internet Address: http://www.equifax.com
- **Experian**
  - Telephone Number: (888) 397-3742
  - Internet address: http://www.experian.com
- **Trans Union**
  - Telephone Number: (800) 888-4213
  - Fraud Line: (800) 680-7289
  - Internet address: http://www.transunion.com

ICBA BANCARD &TCM BANK

Federal Trade Commission (FTC)

- Credit management
- Consumer protection
- Telemarketing fraud
- ID theft affidavit
- www.ftc.gov/idtheft
- 877-382-4357



ICBA
BANCARD
&TCM BANK

Fraud Prevention Measures

- Techniques and Guidelines
- Report Monitoring
- Fraud Patterns
  - Merchant Category Codes (MCC)
- Testing Patterns

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Keep precise records of fraud accounts
  - Use past patterns to guide future actions
  - Report all fraud cases to the proper authorities
  - Require written documentation on all fraud claims
- Incorporate internal and external guidelines to protect your data
  - Require all your venders to give written details of their procedures and software for data protection

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Setup institutional compliance standards based on current legislation and review your policies regularly

- Know your federal, state and local law enforcement offices and their standards for filing criminal reports related to fraudulent or suspicious activity

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Act immediately when your BIN or accounts have been victimized by a fraud attack
  - Use country code blocks
  - Reset parameters
  - Monitor high risk transactions
  - Control payments

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

What Is the Best Defense?

- Know the fraud types and implement prevention measures for each type of fraud
- Educate employees and cardholders
- Monitor reports
- Review all Falcon alerts referred to you
- Have good insurance coverage
- Take appropriate actions to control fraud

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Each institution should establish report monitoring guidelines
  - Determine your “best practices”
  - Set dual controls and passwords
  - Have a cardholder contact plan
  - Have a set policy for blocking and reissuing

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Look for common fraud patterns and testing patterns
- Recent fraud trends and seasonal cardholder patterns should be taken into consideration
  - Christmas holidays
  - Summer vacations
  - Back-to-school

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Expect some "false finds" that appear to be fraud
  - Call cardholders and verify suspicious charges
  - Set timeframes for contacting cardholders
  - Apply a temporary block to avoid further transactions
  - Review the account, closely checking the address and telephone numbers – **KEEP CURRENT INFORMATION**

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Establish criteria for temporarily blocking accounts with or without cardholder verification of transactions
- Keep a list of accounts that exhibit frequent incidents of unusual behavior
- Keep a list of “test merchants”
- Contact your local Postal Inspector for a list of “bad addresses”

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Report Storage
  - Issuers must have a means to store daily files for future reference
    - Securely keep several years of data available for review
    - Always use passwords and dual access controls
    - Establish limits for online storage

ICBA BANCARD &TCM BANK

Fraud Prevention Techniques

- Report Disposal
  - Have a set plan for file disposal
    - Do not leave data on replaced computer systems – always use professional scrubs
    - Never leave discs with report data unprotected
    - Do Not allow unauthorized copies of data
    - Properly destroy old reports and diskettes

ICBA BANCARD &TCM BANK

Report Monitoring

Daily Authorization Reports

Monitoring Field Values

ICBA
BANCARD
&TCM BANK

Report Monitoring

- Most fraud types will be found by checking authorizations report daily
  - Review and understand each field value on this report
  - Remember in many cases fraud may or may not stand out from routine spending patterns
    - You may need to verify past activity using appropriate statement information
- Some fraud types may require additional reports be reviewed

ICBA BANCARD &TCM BANK

Report Monitoring

- **Ten Key Field Values to Review**
  - Daily authorization report
    1. Account number and BIN
    2. Time of transaction
    3. POS entry mode or mode
       - swiped
       - keyed
    4. Expiration date
    5. Authorization amount

ICBA BANCARD &TCM BANK

Report Monitoring

- **Ten Key Field Values to Review (Con't)**
  - Daily authorization report
    6. Response code RSP
       - Approved or declined
    7. Credit available or open-to-buy
    8. Merchant category code or MCC
    9. Merchant name and city
    10. Country

ICBA BANCARD &TCM BANK

Report Monitoring – By Account Number

- Account number
  - How many transactions on the account?
    - Look at any over five
  - Is the account number valid?
    - Several attempts on invalid accounts could be a sign of BIN testing using a Credit Master-type program
- Compare to cardholder history using billing statements – check back several months
- Check for a recent address change, followed by a request for new card to be sent, and request for new PIN

ICBA BANCARD &TCM BANK

Report Monitoring – By Time

- Time is based on a 24 hour clock and EST zone. Look for purchases outside of a normal day for your time zone.
  - Early morning transactions
  - Very late at night
  - After store hours at retailers
  - Transactions a minute or two apart
    - Could be keying error
    - Could be a “testing” pattern

ICBA BANCARD &TCM BANK

Report Monitoring — By POS Entry Mode

- Pos EM or mode
  - O1 manually keyed
  - 90 full magnetic stripe read
  - 02 partial magnetic stripe read
  - 59 electronic commerce transaction
- Watch for numerous POS 01 transactions at face-to-face merchants
- Counterfeit skimming produces 90 reads, but your cardholders will have their cards in their possession

ICBA BANCARD &TCM BANK

Report Monitoring – By Expiration Date

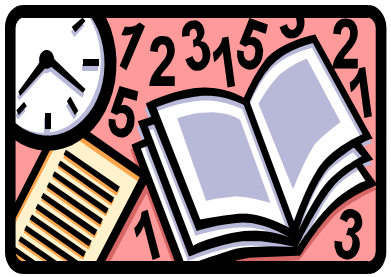
- Expiration date
  - Are there numerous dates used on one account?
  - Are there several accounts with the same date?

- Credit Master or Credit Wizard software will only produce card numbers
    - Perpetrators must guess the expiration date

ICBA BANCARD &TCM BANK

Report Monitoring – By Expiration Date

- Check expiration dates for all suspicious POS 01 transactions
- Expiration dates can be used to determine if a reissued card was used or an original card



ICBA BANCARD &TCM BANK

Report Monitoring – By Amount

- Set a target amount for your card portfolio to check daily
  - Example: all transactions over $2,500.00
  - Cash advances over $1000.00
  - Retail purchases over $5000.00
- Check transactions under $0.99
- Some perpetrators will test an account at one amount one day and a similar amount the next day

ICBA BANCARD &TCM BANK

Report Monitoring – By Credit Avail or OTB

- The credit available and open-to-buy field helps you determine risk
  - Is the account at its capacity?
  - Should you watch for booster payments?
  - Is the perpetrator verifying the account balance through VRU inquiries?
  - How much could be lost by waiting one day to block the account?

ICBA BANCARD &TCM BANK

Report Monitoring – By MCC

- Merchant category codes or MCC's are good indicators of fraud because:
  - Perpetrators often target one or two MCC areas
  - General retail codes are hard to track
  - Always check cash advance or related MCC's
    - 6010, 6011, 6012
  - Note the MCC related to account testing

ICBA BANCARD &TCM BANK

Report Monitoring – By Merchant Name/city

- Merchant name/city
  - Local transactions are the most common
  - Look for large cities (New York, Miami, Las Vegas, Los Angeles, Chicago)
  - Foreign names and/or locations
  - Large banks for cash advances (Citibank, Washington Mutual, Wachovia)
  - Same merchant used on several accounts
  - Blank merchant names or a random series of characters

ICBA BANCARD &TCM BANK

Report Monitoring –
By Merchant Name/city (Con't)

- When a merchant seems to be suspicious and has numerous transactions on your report
  - Call cardholders and verify the transactions
  - Look the merchant up on the internet
  - Contact the merchant directly

ICBA BANCARD &TCM BANK

Report Monitoring – By Country

- Main concerns:
  - Does the pattern match personal or business travel?
  - Is there a history of foreign purchases?
  - Is the activity on several accounts at one merchant?

ICBA BANCARD &TCM BANK

Report Monitoring

Using Report Filters

- When reviewing reports, issuers can filter for one field or field value to review those transactions

- Recommended daily filters:
  - Cash advances
  - Large transactions over $3000.00
  - Wire transfers
  - Non-local transactions
  - Special declines

ICBA BANCARD &TCM BANK

MCC 6010 Filter

Monarch - 20050915-CP211004.prf - CP211004-1.PRN, Auth Report Model ... - [Table]

File Edit Data Options Window Help

Courier 10

	EXPR	AUTH	BL	CRED L	CRED A	PO	CTR	CIC	VV	P	DATE	TIME	ACQUIRE	MERCHANT	MF	MCC	UTH N	RS	DCL	AMOUNT
89	1007	0		4000	2160	90	US	22			09/15	10:49	475541	KEYBANK 2023 N O	CA	6010	00000	51	607	2400.00
90	1107	0		10000	1558	0	US	–			09/15	17:07	0		C	6010	01146	00	000	1000.00
91	1107	0		2500	1304	2	US	21			09/15	17:36	460443	TEACHER FEDERAL	C	6010	08320	00	000	200.00
92	1207	0		7500	698	90	US	21			09/15	16:21	440140	WASHINGTON MUTUA	CA	6010	0 0000	51	607	1127.51
93	1107	0		12000	187	90	US	21			09/15	14:41	440140	WASHINGTON MUTUA	CA	6010	0 6113	00	000	550.00
94	0208	0		10000	9415	90	US	22			09/15	16:14	423342	COAST CENTRAL 04	CA	6010	07453	00	000	100.00
95	0406	0		7500	4774	90	MX	22			09/15	15:14	493700	SBIT 389 ZONA DO	CA	6010	04039	00	635	281.11
96	0608	0		3000	240	0	US	–			09/15	17:16	0		CA	6010	06110	00	000	240.00
97	0608	0		3000	70	90	US	21			09/15	14:46	449280	BANK OF AMERICA	CA	6010	02539	00	000	250.00
98	0708	0		7500	1410	0	US	–			09/15	17:16	0		CA	6010	00452	00	000	500.00
99	0408	0		8040	7740	90	AW	22			09/15	13:07	492032	ARUBA BANK N V C	CA	6010	00710	00	635	300.00
100	0608	0		11025	2182	90	US	21			09/15	12:21	449280	BANK OF AMERICA	CA	6010	00221	00	000	3000.00
101	1205	0		1125	519	90	US	21			09/15	09:59	482099	MUNICIPAL CU-QUE	CA	6010	00447	00	000	600.00
102	0607	0		7500	3520	90	US	21			09/15	17:07	482099	MUNICIPAL CU-QUE	CA	6010	00510	00	000	1000.00
103	0908	0		9675	3705	90	US	21			09/15	11:49	482099	MUNICIPAL CU-BRO	CA	6010	00765	00	000	1000.00
104	0208	0		5775	173	90	US	21			09/15	12:43	482099	MUNICIPAL CU-BRO	CA	6010	00463	00	000	300.00
105	1007	0		10125	5528	90	US	22			09/15	14:10	475542	WACHOVIA BORDEAU	CA	6010	00002	00	000	368.86
106	0108	0		2700	535	1	US	–			09/15	10:10	442513	CITIBANK, FSB #2	CA	6010	00655	00	000	250.00
107	0808	0		4275	493	90	US	21			09/15	16:58	482099	MUNICIPAL CU-BRO	CA	6010	00607	00	000	2000.00
108	1006	0		1875	251	90	US	21			09/15	11:24	482099	MUNICIPAL CU-BRO	CA	6010	00452	00	000	70.00
109	0808										09/15	09:43	482099	MUNICIPAL CU-BRO	CA	6010	00662	00	000	150.00
110	0208										09/15	10:08	475542	FIRST PENN BANK	CA	6010	00539	00	000	80.00
111	0607										09/15	12:57	840200	COMMERCIAL BANK	CA	6010	00919	00	000	2500.00
112	0207										09/15	11:14	482099	WEST MICHIGAN CU	CA	6010	00816	00	000	200.00
113	0206										09/15	17:16	0		CA	6010	00604	00	000	300.00
114	0707										09/15	17:07	0		CA	6010	00620	00	000	184.00
115	0706										09/15	17:16	0		CA	6010	00679	00	000	277.00
116	0207										09/15	10:06	407063		CA	6010	00143	00	000	600.00
117	0406										09/15	17:35	482099		CA	6010	00656	00	000	157.50
118	0407										09/15	17:16	0		CA	6010	04319	00	000	890.00
119	1207										09/15	11:28	482099	SAFE FEDERAL CU	CA	6010	01664	00	000	50.00
120	0809										09/15	15:53	482099	SAFE FEDERAL CU	CA	6010	02654	00	000	100.00
121	1106										09/15	11:58	482099	OAKLAND CO ECU W	CA	6010	05529	00	000	1000.00
122	0507										09/15	16:47	482095	BULLS EYE CREDIT	CA	6010	08371	00	000	520.00
123	1105										09/15	16:43	412163	FIRST BREMEN BAN	CA	6010	05260	00	000	1200.00
124	1005										09/15	09:39	871300	COMMODORE BANK #	CA	6010	03749	00	000	500.00
125	0906										09/15	16:33	412163	FIRST BREMEN BAN	CA	6010	04345	00	000	4500.00
126	0707										09/15	13:32	482099	TOLEDO AREA COMM	CA	6010	03405	00	000	500.00
127	0207										09/15	17:37	482099	TOLEDO AREA COMM	CA	6010	02101	00	000	700.00
128	0806										09/15	17:07	0		CA	6010	08222	00	000	500.00
129	0906	0		8680	1385	0	US	–			09/15	17:07	0		CA	6010	05494	00	000	2500.00
130	0807	0		7000	879	2	US	22			09/15	15:11	460594		CA	6010	02056	00	000	250.00

Filter: New CA Sort, Sort: Account

Filters allow you to focus on one field to identify related accounts

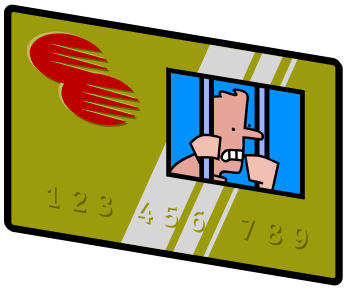
Fraud Patterns

ICBA
BANCARD
&TCM BANK

Fraud Patterns

Characteristics of Fraud

- Foreign transactions
- POS 90 (skimmed transactions)
- Large dollar
- Test transactions appear prior to fraud
- Transaction out of the cardholder's community



ICBA BANCARD &TCM BANK

Fraud Patterns

- Sudden shifts in merchandise purchased
  - Sharp increase in purchases
  - Business items to personal items
- Suspicious or excessive purchases by
  - Volume, timing, MCC, or group code
- Retail purchases over $250.00
  - Jewelry or designer items
- Purchases over $1000.00
  - Merchant group codes: EL, DS, JS, & CA
    - Electronics, Discount Stores, Jewelry Stores, Cash Advances

ICBA BANCARD &TCM BANK

Fraud Patterns

- Large or multiple cash advances
- Multiple internet, mail, or telephone purchases in a short time frame
- Various POS 90 authorizations in multiple cities and various locations
- Extremely high dollar amount payments

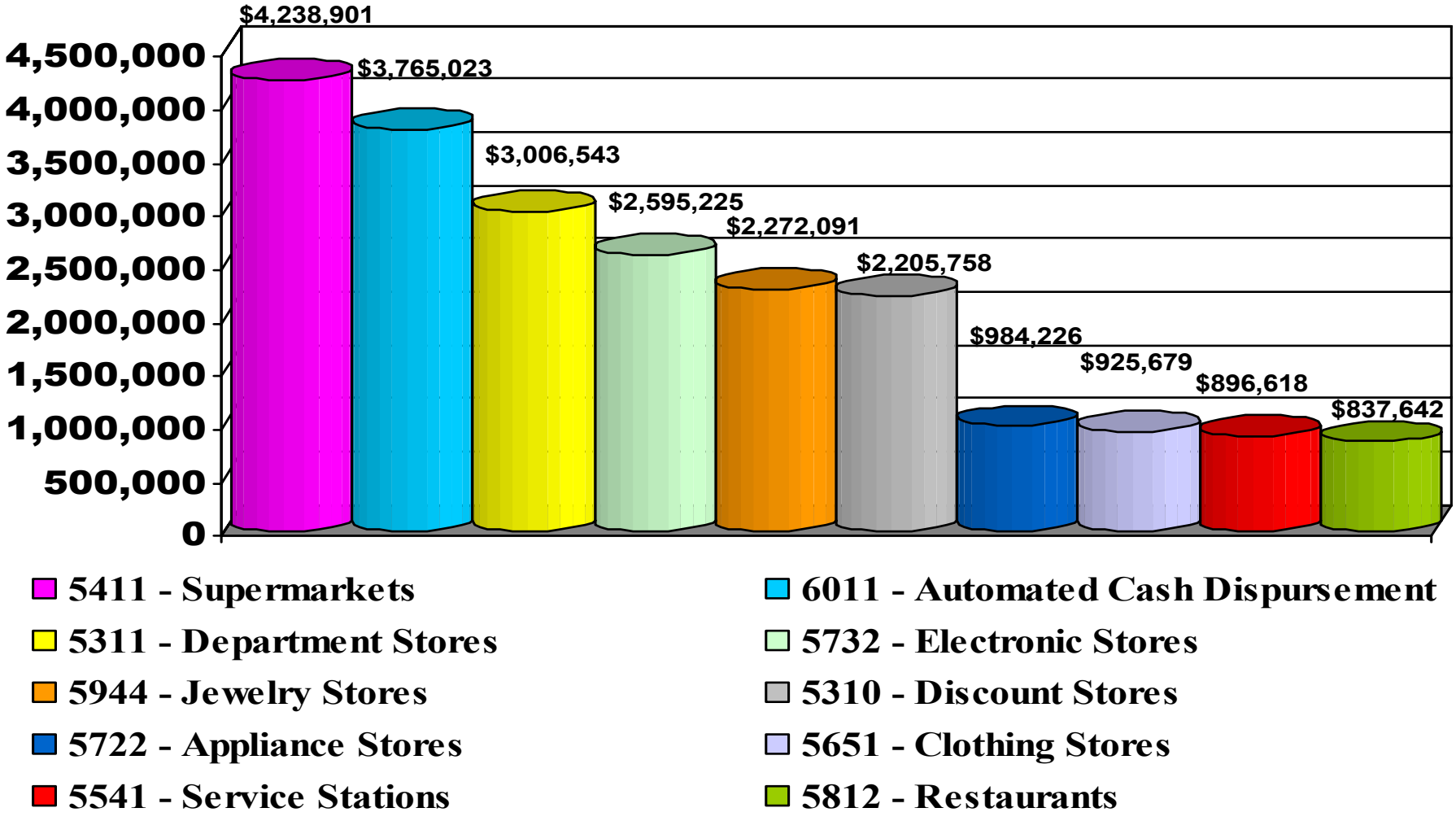
ICBA BANCARD &TCM BANK

Merchant Category Codes (MCC)

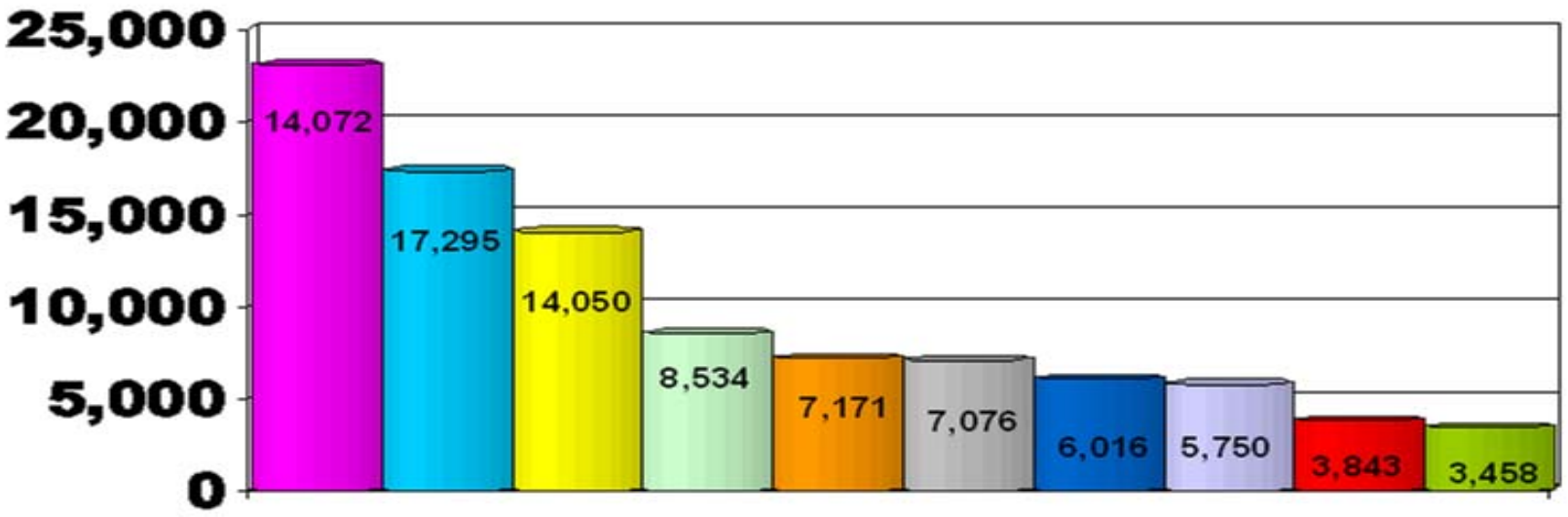
- Perpetrators tend to use the same techniques and often the same merchants
- Monitoring all transactions in a MCC group can help control fraud
- Awareness of current testing patterns can help you isolate that activity via the MCC

ICBA BANCARD &TCM BANK

Top 10 MCC's by Fraud Dollar Amount



Top 10 MCC's by Transaction Volume



- 5542 - Automated Fuel Dispensers
- 5541 - Service Stations
- 5812 - Restaurants
- 4784 - Toll & Bridge Fees
- 5912 - Drug Store/Pharmacy
- 5411 - Supermarkets
- 5311 - Department Stores
- 5310 - Discount Stores
- 5814 - Fast Food Restaurants
- 6011 - Automated Cash Disbursements

High Risk Countries

- 1. United Kingdom
- 2. Romania
- 3. Canada
- 4. France
- 5. Australia
- 6. Mexico
- 7. Philippines
- 8. Italy
- 9. Israel
- 10. Malaysia
- 11. Japan
- 12. Korea
- 13. Turkey
- 14. Germany
- 15. Hong Kong
- 16. Russia/Ukraine

ICBA BANCARD &TCM BANK

***These high risk countries are subject to change**

Testing Patterns

Characteristics of “Testing” Top Test Merchants

ICBA
BANCARD
&TCM BANK

Testing Patterns

- Account “testing” normally consists of small authorizations which are made to verify that an account number is usable
  - Test transactions may lead to fraud immediately
  - Fraud may be delayed for several months
  - There may never be fraud

ICBA BANCARD &TCM BANK

Testing Patterns

- Test authorizations normally never post to the account
- Test authorizations often lead to subsequent fraud at a different merchant
- Test merchants may not be aware of the fraud

ICBA BANCARD &TCM BANK

Testing Patterns

- "Test" authorization characteristics
  - Multiple 01 transactions at several merchants
  - Multiple invalid account number declines
  - Excessive authorizations minutes or seconds apart

ICBA BANCARD &TCM BANK

Testing Patterns

- "Test" authorization characteristics
  - Various expiration dates are used with the same account number
  - Small dollar purchases at the same merchant using several account numbers
  - Authorizations for $.99 or less
  - Recent trends reflect that test transactions are made at higher dollar amounts to avoid detection

ICBA BANCARD &TCM BANK

Popular Test Merchants

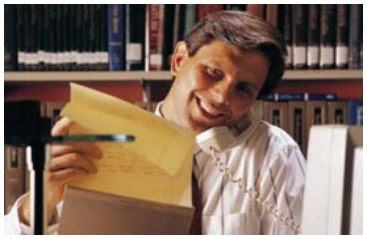
- 1-800-Flowers.com (MCC 5992)
- 2B Sport (MCC 5695)
- Abnet Com (MCC 7372)
- Formento Gastronomico (MCC 5812)
- MFI*MyFamily/Ancestrys (MCC 4816)
- Racing Bag.com (MCC 2741)
- Allegro Medical (MCC various)
- Apple Store (MCC various)
- Kodak (MCC various)
- Daniel's Moving & Storage (MCC 4225)
- 'Random alpha characters' (MCC various)
- Blank merchant name field (MCC 5999 & 4225)

***These test merchants are subject to change**

ICBA BANCARD &TCM BANK

Sources for Known Fraud Patterns

- Falcon alerts
- Visa CAMS or MasterCard Alerts
- Association meetings - information sharing
- Current news articles
- Current fraud cases



ICBA BANCARD &TCM BANK

Current Industry Fraud Initiatives

FIS»
FIDELITY NATIONAL INFORMATION SERVICES
&TCM BANK

Neural Network Enhancements

- Real Time Decisioning –Additional Core Feature of Neural Network Solution
  - Ability to Prevent Fraud at Point of Sale
  - Ability to Send Selected Population of Transactions for Decisioning
    - Target Foreign Transactions
    - Target Specific Merchants
    - Target Flash Frauds
  - Increased Usage of Rules to Tune False/Positives

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

Neural Network Enhancements

- Additional Scoring Rules provided by Visa Advance Authorizations product
- Allows for Stand Alone Servicing
- Fraud Predictor Option to Include Merchant Profiles
- Debit Split Profiling- PIN vs. Signature

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

Visa's ADCR Program

Visa's Account Data Compromise Recovery Program

- Took affect October 1, 2006
- Replaces the old recovery process that was in place, and has no affect on events prior to this date
- Provides partial recovery for magnetic-stripe counterfeit fraud only and operational expenses

ICBA BANCARD &TCM BANK

Visa's ADCR Program

- Program Qualifications:
  - An account compromise event has been confirmed
  - A CAMS alert has been distributed to Issuers affected by the event
  - Full magnetic stripe information was obtained, and swiped counterfeit card fraud resulted
  - The confirmed event involved a minimum of 10,000 US Visa account numbers
  - Visa has determined that above baseline fraud has occurred as a result of the event

ICBA BANCARD &TCM BANK

Visa's ADCR Program

Make sure you are…

1. receiving CAMS Alerts

2. enrolled to recoup operational expenses
   - Use Visa Online to enroll in program; including Ops expenses

- Reporting your fraud correctly to Visa

Reimbursement is automatic in the event of a compromise.

- Operational expense reimbursement typically $1 per exposed account if VISA determines POS 90 counterfeit
- Fraud loss reimbursement is based on 13 months of loss experience due to counterfeit

ICBA BANCARD &TCM BANK

Dynamic Magstripe
Overview

Card authentication solution that protects against counterfeit and renders data useless if compromised

- Applicable in all magstripe terminals
- Targeted for deployment in high risk card types
- Delivers dynamic data using the existing magnetic stripe infrastructure

DM Card is Swiped

Works with standard terminal

Dynamic Magstripe Card Verification Value

Helpful Websites

www.pcisecuritystandards.org

info@pcisecuritystandards.org

www.visa.com/cisp

cisp@visa.com

www.merchant911.org

www.ftc.gov

ICBA BANCARD &TCM BANK

FIS Fraud Initiatives

FIS
FIDELITY NATIONAL
INFORMATION SERVICES
&TCM BANK

FIS Major Card Fraud Initiatives

- Compromised Account Solution
- Communication & Education
  - www.fisriskmanagement.com
- Secure Debit / Secure Credit

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

Compromise Manager

- Auto Feed of Alerts from Visa and MasterCard
- Account monitoring
    - Account Flagged with Date/Event#/Severity Level
    - Account Memos for all related activity
    - Ability to Monitor in Neural Network
- Immediate Card Blocking
- Delayed Blocking
    - Reissue New Card
    - Current Card Still Valid Until Customer Card Activates New Card
    - Card Activation Integration

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

Compromise Manager

- Reissue Management
  - Putting Cardholder Data in front of client on a screen to assist in reissue decision
    - Data Elements: Account number, Cardholder Name, Last Date of Activity, Status, Open to Buy/Available Balance, Last Reissue Date, Card Activation Status, Expiration date, Last Payment Date
    - Ability to Download Event Information for Review Internally
    - Ability to Upload Accounts into Utility in Excel after review
- Cardholder Notification
    - Letters (Generic or Customized)
    - IVR for Immediate Blocked Accounts
- Availability- PT, BASE2000 and TBS 1Q '07

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA
BANCARD &TCM BANK

Education and Communication

- Fraud Communication Website Q1 ’07 (www.fisriskmangement.com)
  - Fraud trends
  - Fraud alerts/ interactive between FIS and clients
  - Tips and best practices
  - Repository for test merchants, bad addresses
  - Fraud product updates

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

How can FIS help you with reducing Fraud?

Secure Debit Program

VISA

MasterCard

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

What does Secure Debit cover?

- Secure Debit indemnifies credit unions from the following debit card losses:
  - Mail intercepted / Never received as issued – cards sent out are intercepted
  - Lost / Stolen cards with unauthorized use - 50% of all fraud
  - Counterfeit / Skimming - most dangerous and expensive fraud types
  - Unauthorized Use and Phishing/Pharming to attain card information to include PIN compromise

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

What are the benefits of Secure Debit?

- Provides reimbursement for any losses over $50 per occurrence with caps on coverage
- Helps customers realize greater fee/interchange income
  - In some cases, as much as 120%
  - Impacts bottom-line profitability
- Provides your institution with peace of mind for any fraud associated with your debit card program
- Decreases check processing costs

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

What is not covered?

- Employee theft or negligence
- Friendly fraud
- PIN disclosures
- VIP card status
- Any transactions that are proven to be out of compliance with our processing requirements

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

What are the Processing Requirements?

1. **Falcon with Falcon Expert Rules – cardholder contact & blocking decisions performed by FIS**
2. **CVV/CVC - decline for a mismatch on all PIN and Signature transactions**
3. **CVV2/CVC2 - decline for a mismatch on all Signature transactions with CVV2/CVC2**
4. **3-D Secure (Verified by Visa or MasterCard SecureCode) - auto-enrollment**
5. **Expiration Date Matching – decline for a mismatch**
6. **Card Activation - all new or reissued cards require card activation (VRU or 1st PIN)**
7. **Authorization Name Matching – recommended**
8. **Required Card Limits**
    a. **Daily ATM Limit – up to $510 per account per day**
    b. **Daily Purchase Limit – up to $1,500 per account per day**
    c. **Daily Cash Advance Limit – up to $1,000 per account per day**
9. **Address Verification Service (AVS) – required & performed by FIS or client's host system**
10. **Principal Members – must send Alerts (compromised account) information to FIS**
11. **Chargeback Processing - FIS performs basic or enhanced chargeback processing**

ICBA BANCARD &TCM BANK

How much does it cost and when can I get started?

- Pricing Based on percentage of Gross Sales Volume
  - Falcon Case Mgt Fees - Waived
  - Chargeback Fees for Fraud Recovery – Waived
- Rollout Approach
  - Product available Now
  - Existing contract amendment will be provided in order to add the service
  - Two week lead time for implementations

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

Secure Credit

- Modeled after Secure Debit
- Directed specifically to the Credit Card application
- Will apply to all configurations:
  - Full Service Credit
  - Pass Through Credit
  - Self-Administered Credit
- Available 4th quarter of 2006

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

Additional Fraud Development Opportunities

- Card Activation Enhancements
- FIS Neural Network Enhancements
  - Point of Compromise Detection
  - Merchant Profiles
  - Client-level Thresholds and Service Levels
- Anti-Phishing Solution
- Fraud Consultation and Training
- Parameter Reviews and Certification

FIS
FIDELITY NATIONAL INFORMATION SERVICES

ICBA BANCARD &TCM BANK

Fidelity Fraud Prevention Resources

- FIS Risk Management Website
  - www.fisriskmanagement.com
- Fraud Prevention Hot-line:
    - 1-800-282-7629
- Fraud Prevention email box:
    - Cardfraud@fnis.com
- Fraud Prevention Reference Guide
- Fraud web training classes
- Fraud Prevention CBT:
  - Issuer Fraud Awareness
  - Identity Theft

ICBA BANCARD &TCM BANK

Questions

- Contact information:

  Alan J. Nevels

  ICBA Bancard, Inc

  202-821-4317

  800-242-4770

  Fax: 202-659-3606

  Alan.Nevels@icba.org

- Contact information:
  - Brian Mills
  - Fidelity National Information Services (FIS)
  - 800- 282-7629
  - Fax: 727- 227-5437
  - Brian.Mills@fnis.com

ICBA BANCARD &TCM BANK