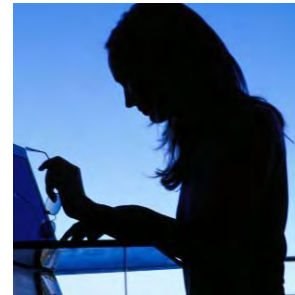
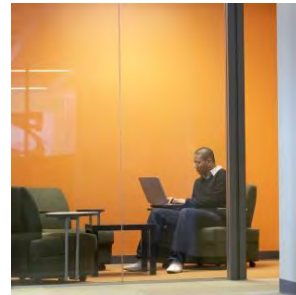


Risk Management: Your Performance in a Soaring Fraud Climate

JB Rambaud
GM Risk Solutions

Agenda

- **Industry Outlook**
 - Challenges
 - Opportunities
- **Fiserv Risk Outlook**
 - Your Fraud Trend
 - Your Fraud Performance
- **Our Strategy – Improve Performance**



Industry Outlook

Key Challenges for Financial Institutions

- **Fraud continues to be a big issue**
 - In 2009, fraud losses to financial institutions were **7.5 basis points** for signature debit and **1.0** for PIN debit
 - In 2008, signature debit fraud losses totaled **5.2** and PIN debit at **.8** basis points
- **Federal regulation threatens to impact revenue**
 - Consent for overdraft protection programs
 - Debit card programs may see less approved transactions, and lower interchange income

A Financial Institution with \$100 million in debit card spending would lose \$75,000 in fraud losses at 7.5 basis points

Pulse Network 2010 Debit Issuer Study

Data Breaches Contributing to Fraud

- **Financial Institutions involved in data breaches**
 - Total of 62 breaches in 2009
 - 1st quarter of 2010, 25 breaches reported compared to 19 from the year before
 - 4.7% increase
 - Total of 37 breaches as of June 2010
- **How is the data breached?**
 - Insider theft was the primary contributor in 2009
 - Outside network intrusion followed by stolen or missing hardware in 2010

2010 Data Breach report by the Identity Theft Resource Center

The “Big” Business of Fraud

Top Five Fraud Threats for 2010

- **Malware attacks**
 - Worms, trojans, and botnets (oh my!)
- **Advanced phishing, vishing, smishing and whaling**
 - Increasing number of attacks on social networking sites
- **ATM skimming**
 - In Las Vegas, 75 skimming attacks reported within 3 month period compared to one or two incidents a year
- **SQL injections**
 - Stealing database information and hacking web sites
- **Counterfeiting in non-EMV countries**
 - Higher fraud rates for non-EMV countries

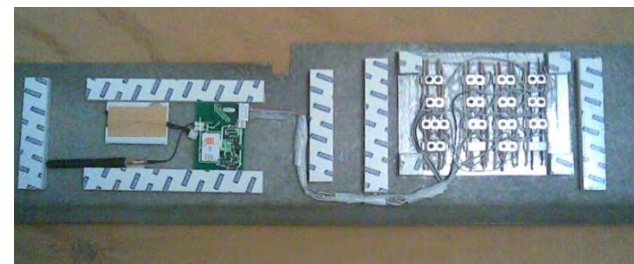
More Sophisticated Attacks

Compromise of ATM PIN Transactions

- **Beginning in 2008, ATMs became the target of malware attacks**
 - Malware (malicious software) installed on ATMs with the purpose of obtaining full-magnetic stripe and PIN data
 - Organized criminal groups may be responsible for the development of the malware
 - Malware is loaded using USB drives
- **Attacks have been reported in Russia and the Ukraine, and more recently in the US**
- **ATMs located in non-bank locations**
- **Two primary versions of the malware designed to take advantage of Diebold and NCR ATMs**
- **Impacted ATMs were not using PCI or PCI-approved encrypting PIN pads**

Example of ATM Attacks

- To upload the malware, fraudsters used USB drives
- Fraudsters had attained administrative access to the ATM platforms operating system
- Fraudsters inserted specially encoded cards into the ATM card reader to retrieve the compromised data
- Dependent upon contents of the card, the criminals low-level employee (mule) was given up to ten choices off the malware menu
- Hardware kit provided by Russian mafia to fit ATM models



Changing Fraud Behavior

- **Fraudsters will continue to use social engineering techniques to target social networking sites**
- **Areas of risk for account takeover and malware plants on unsuspecting users PCs:**
 - Dating sites
 - Classifieds
 - Games
 - Facebook, Twitter
- **A phishing trip that deceives and manipulates the user can prove rewarding to the fraudster**
- **The user is tricked into providing account data which paves the way for cross-channel fraud**



Social Engineering Targeting the Social Networks



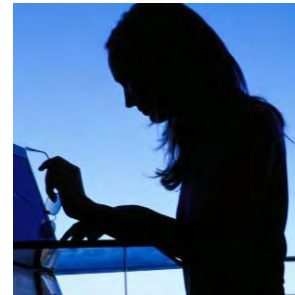
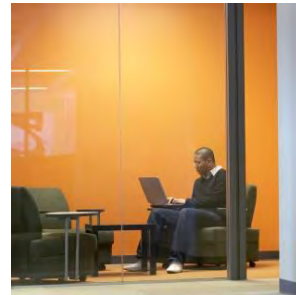
twitter



Opportunities for Growth in 2010?

- **Debit consumer and business card both showed increased usage**
- **PIN debit transaction growth predicted to increase by 9%**
- **Signature debit predicted to increase by 8%**
- **Potential revenue opportunities with Rewards programs and gaining the attention of the small business owner**
- **The economic shift and new regulations have impacted customer behavior**
- **Cardholders are spending less on credit and shifting to debit**
 - Cardholders want a product that does not allow borrowing
 - Ease of use and convenience
 - Credit lines have decreased or closed

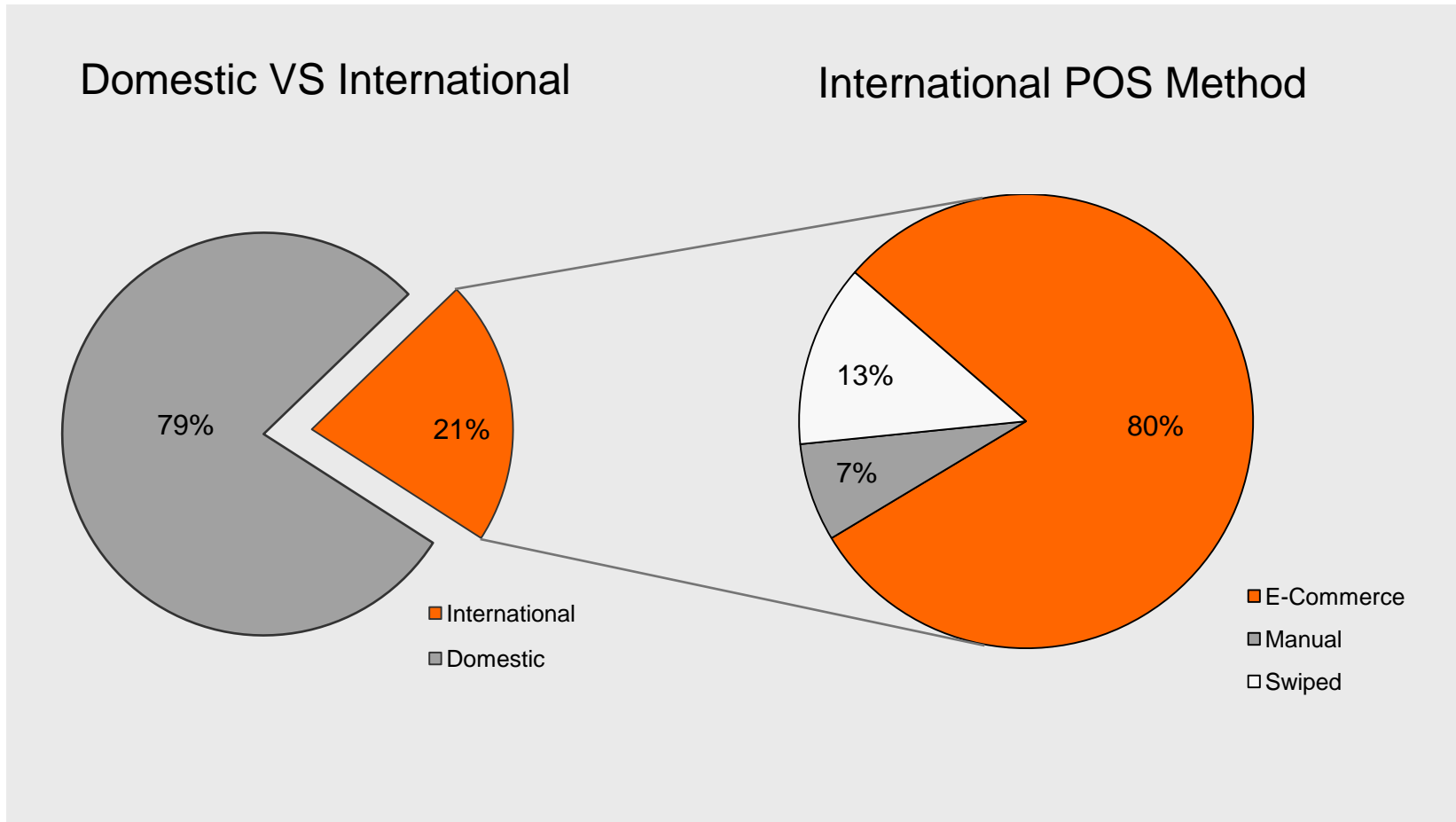
Pulse Network 2010 Debit Issuer Study



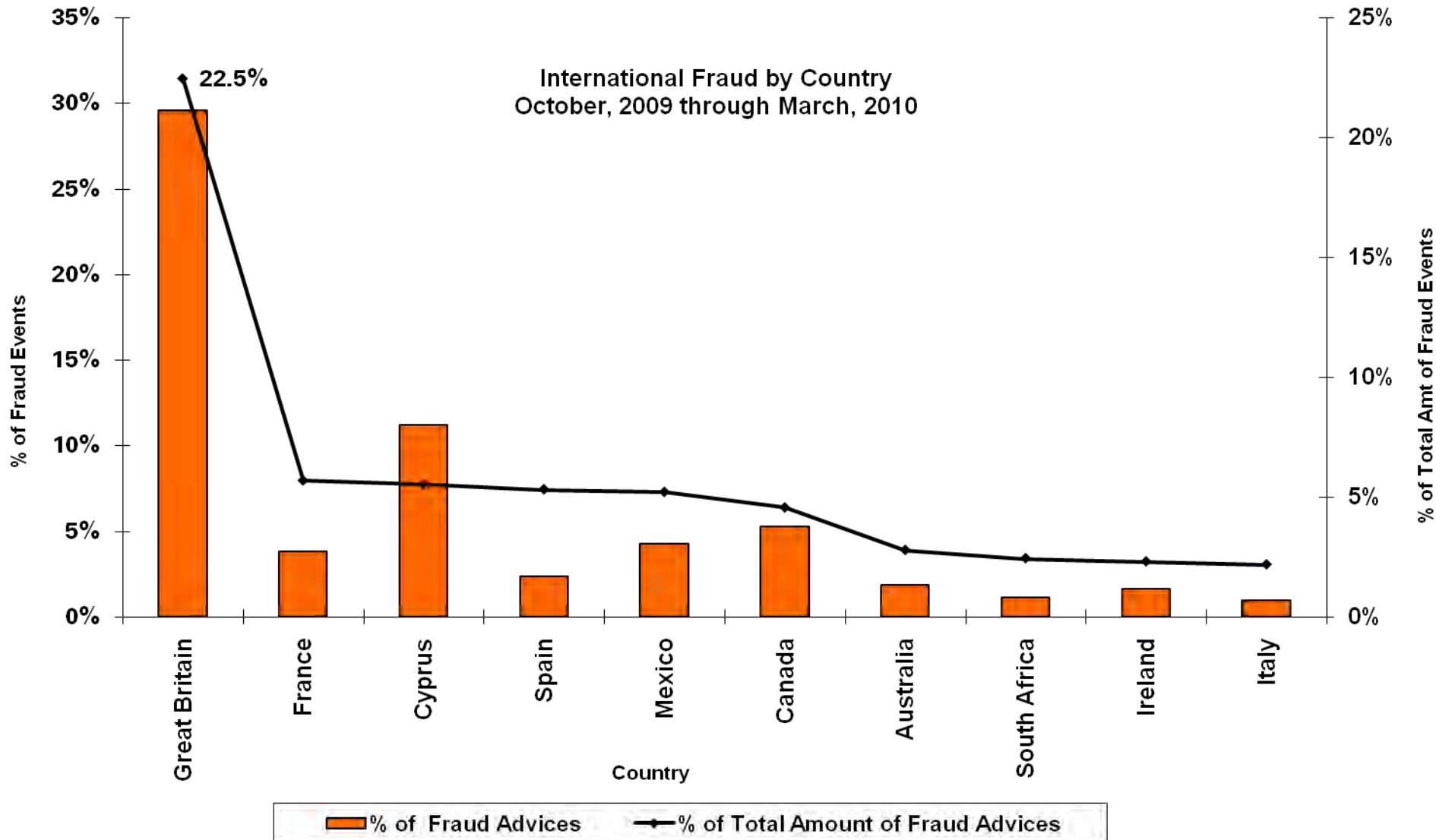
Fiserv Risk Outlook

Reported Fraud Analysis

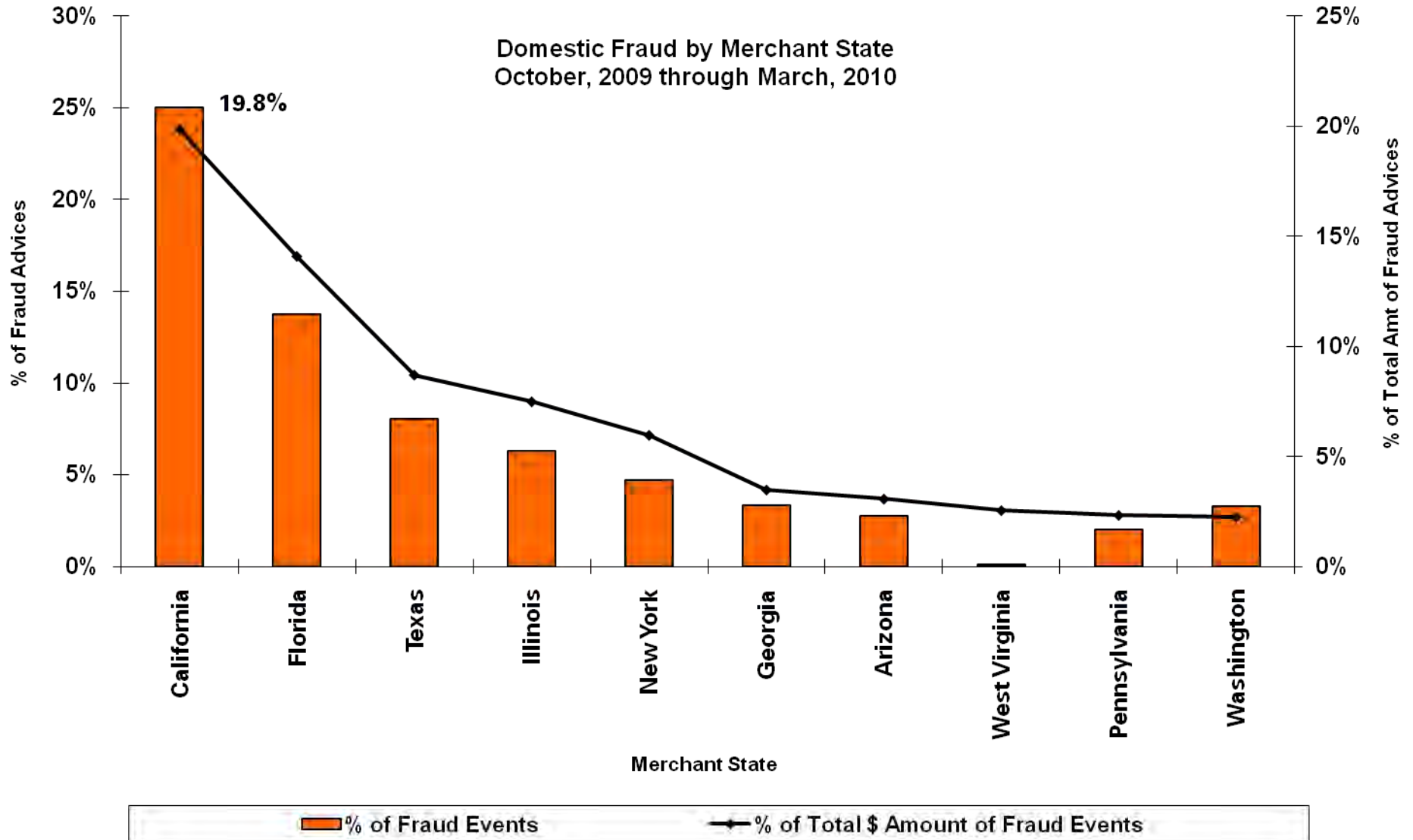
How Much of the Fraud Is Occurring in the US?



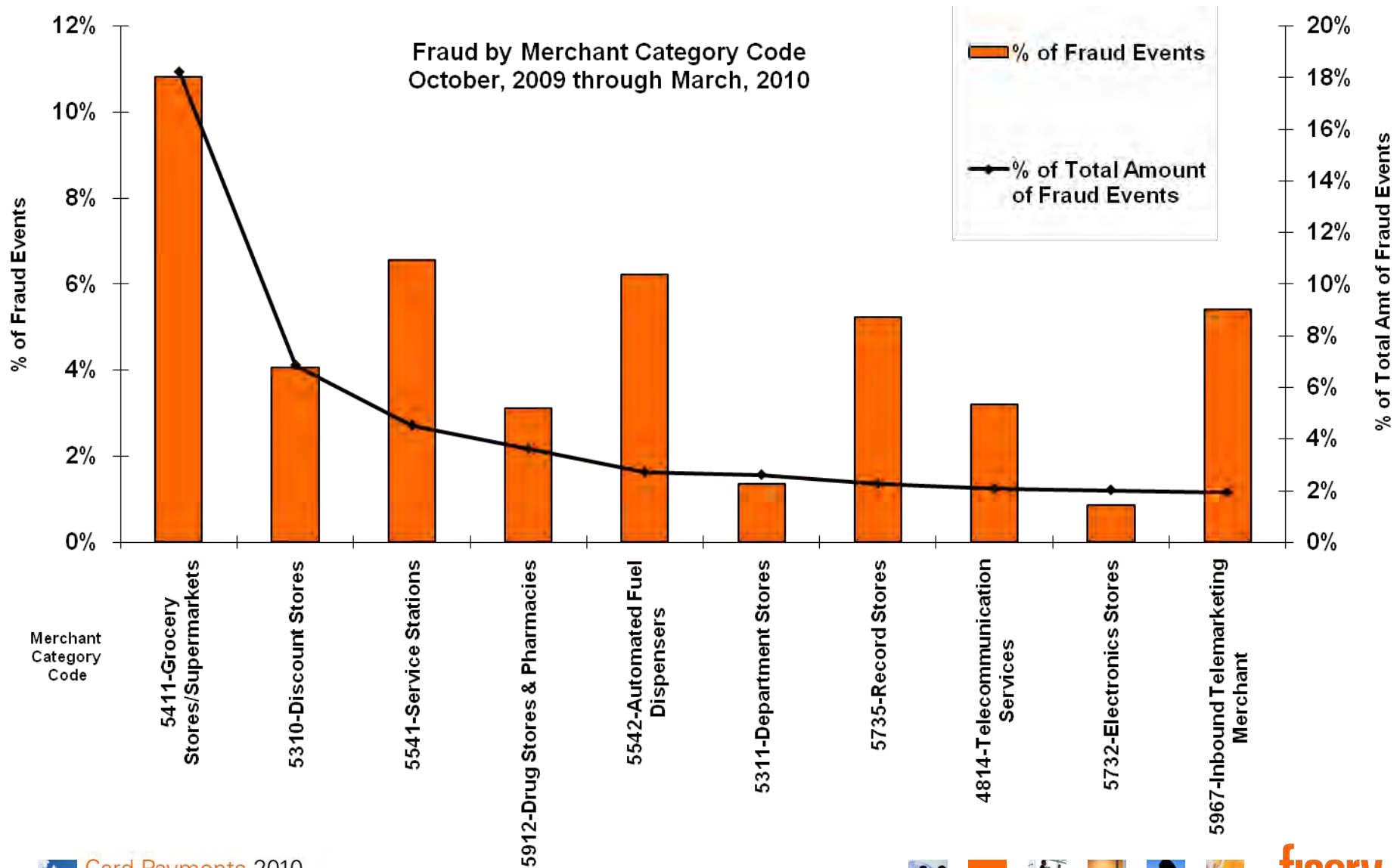
Fraud by International Country



Fraud by US State

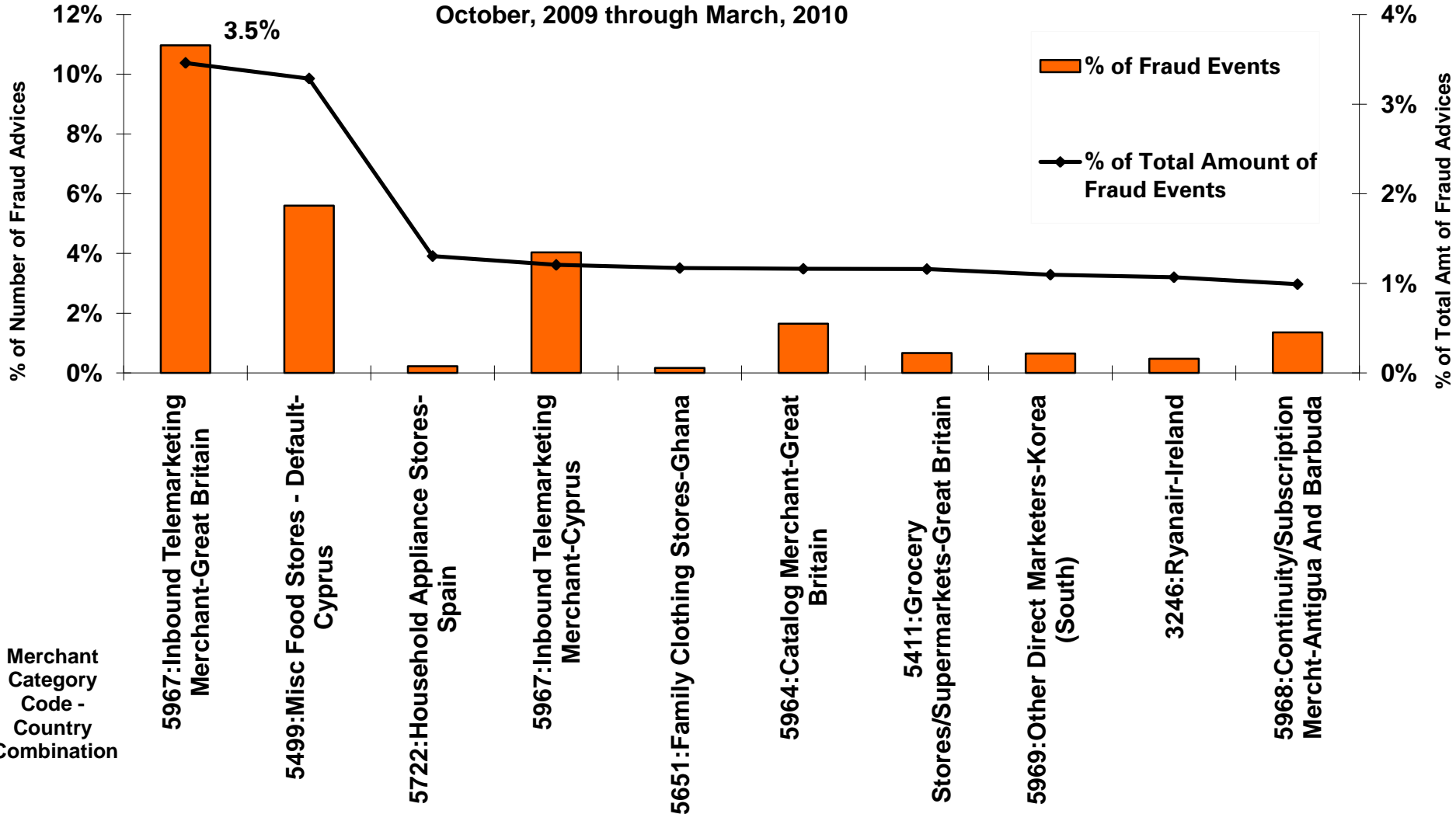


Fraud by Merchant Category Code



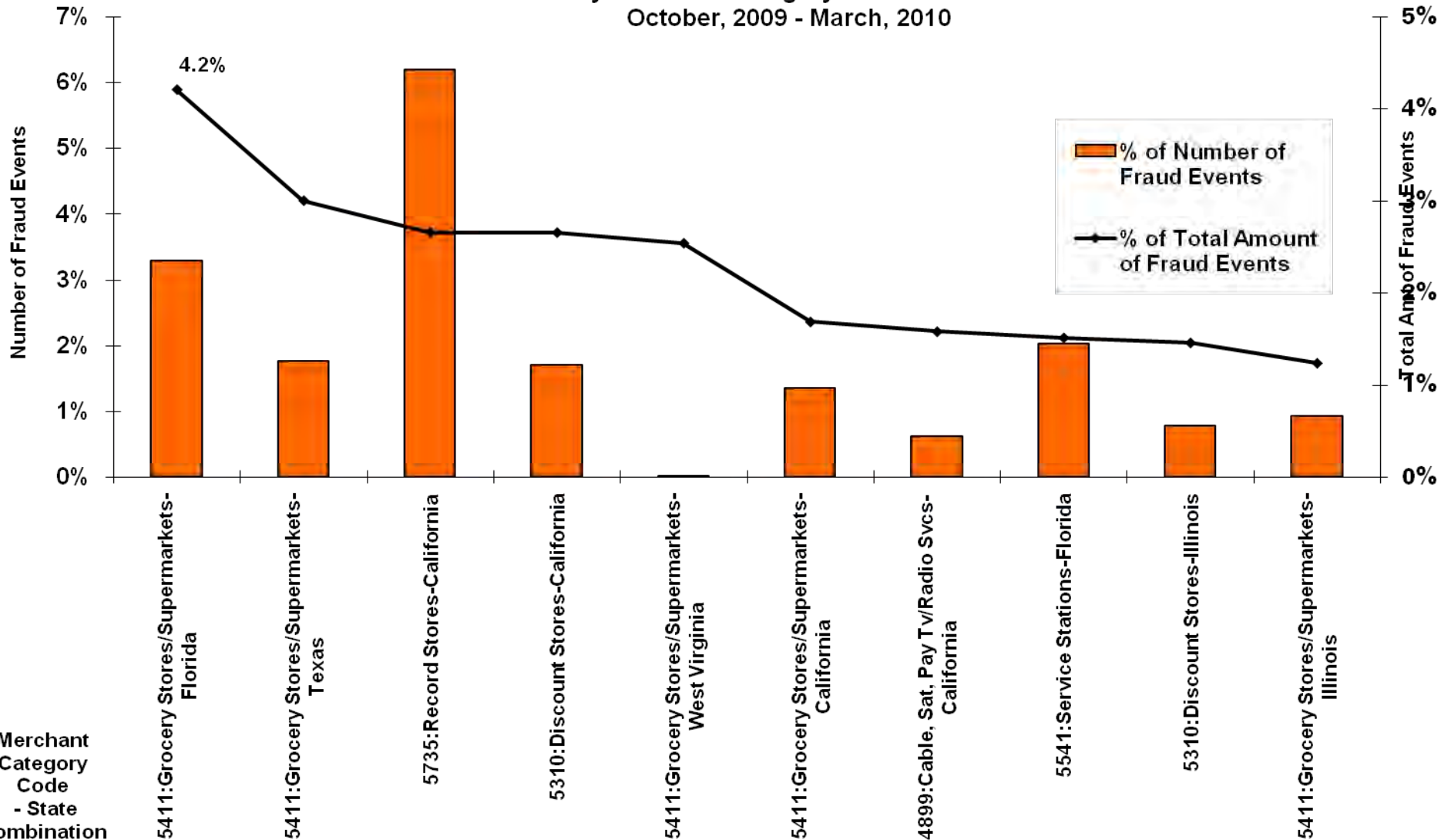
Fraud by MCC/Country Combination

Fraud by Merchant Category Code / Country Combo
October, 2009 through March, 2010



Fraud by MCC/State Combination

Fraud by Merchant Category Code \ State Combo
October, 2009 - March, 2010



Merchant Category Code - State Combination

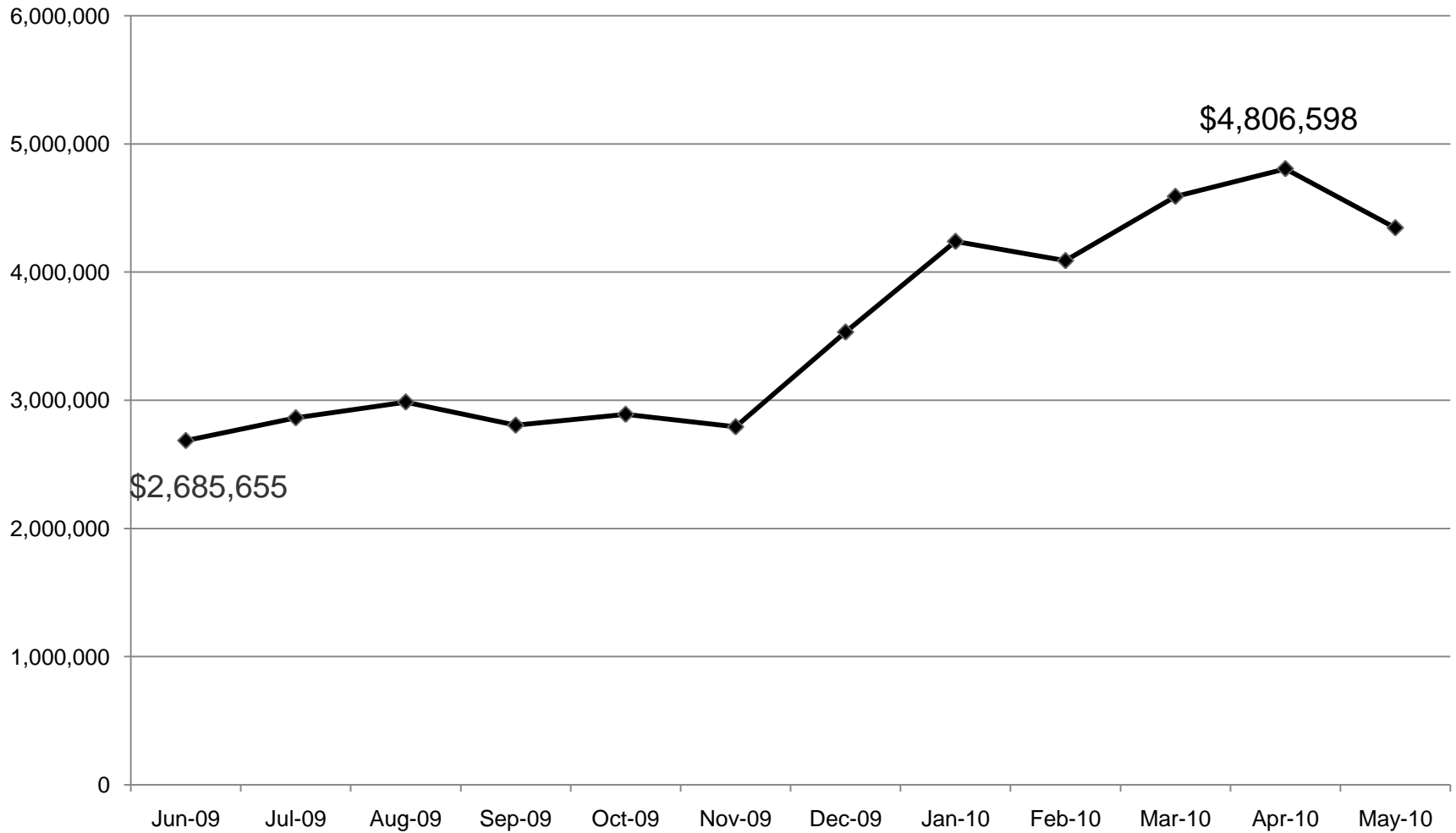
Risk Market Performance vs. Fiserv Risk Performance

- Clients not utilizing Fiserv Risk Solutions have an average of **7.96** basis points of fraud loss
- The risk market average of fraud losses to total transaction dollars is **7.5** basis points (from 5.2 in 2008)
- Clients utilizing the **FULL** Fiserv Risk Solution suite of products and services have an average of **2.89** basis points

Leverage Fiserv Risk Solutions to manage risk

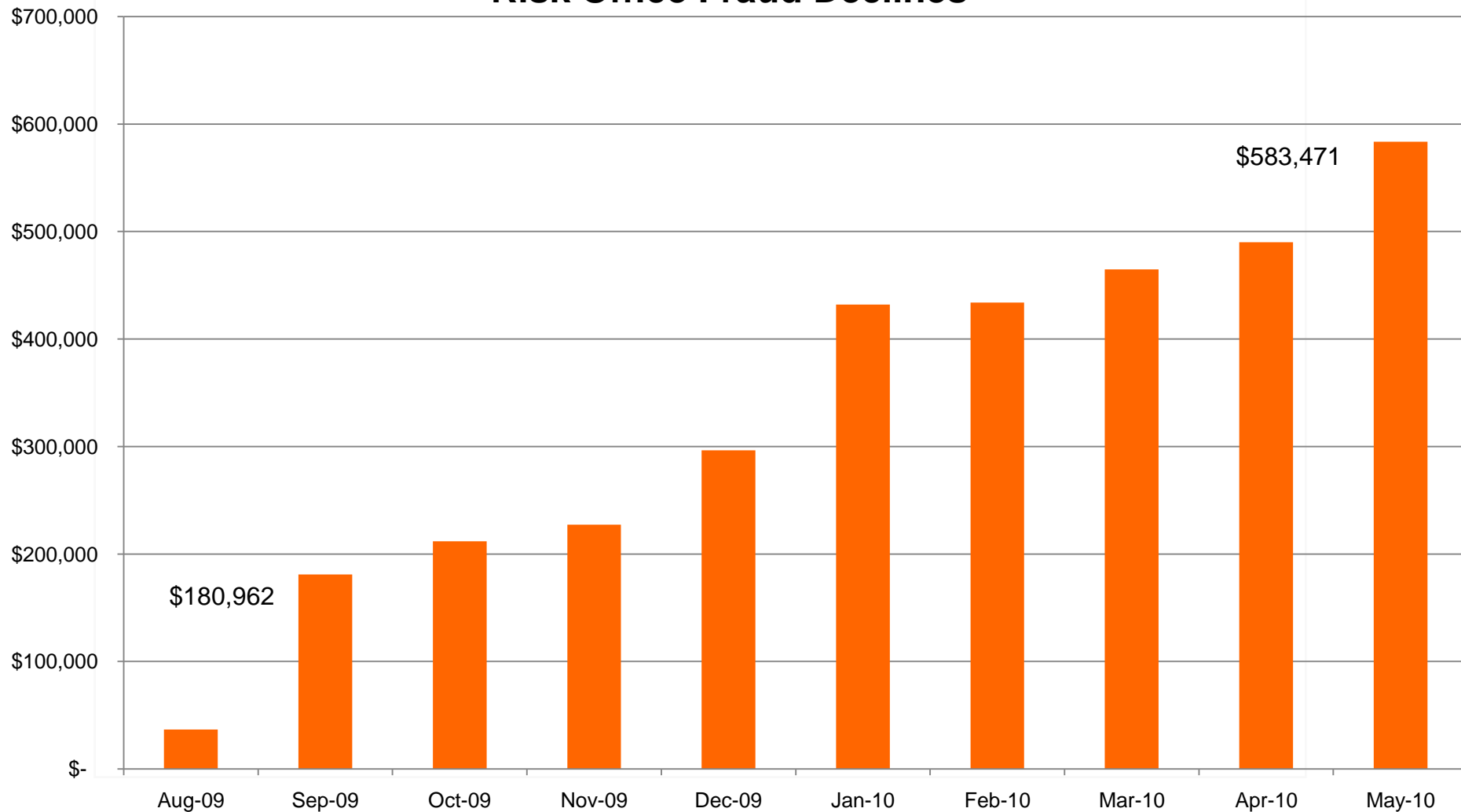
Your Recent Reported Fraud

Total Client Reported Fraud



But Risk Office Stops Fraud For You !

Risk Office Fraud Declines



Fraud Moves Quickly

Closer Look at Some Recent Fraud Patterns

February 2010

Domestic:

MCC 7372 – Direct Marketing –
Inbound Telemarketing
Merchants

Declined 282 Attempts

March 2010

International:

Antigua & Barbuda
MCC 5968 – Continuous
Subscription Merchant

Declined \$12,210 in Attempts

April 2010

International:

Great Britain – St. Kitts/Nevis
E-commerce

Declined 312 Attempts

May 2010

Domestic:

MCC 3048 – Royal Air Maroc
AIRMARO

Declined 7 Attempts for \$6,561

Current Rule Performance

The More Tools You Have Available and Ready, the Better

Rule Name	False Positive Ratio
• CardTracker	7.83 to 1
• TranBlocker	5.16 to 1
• Fraud Score	4.87 to 1
• Fraud Score & CardTracker	2.90 to 1
• CardTracker & TranBlocker	2.37 to 1
• Fraud Score & Real-Time	2.13 to 1
• Real-Time & CardTracker	1.19 to 1

When multiple tools are in place you will see efficiency increase dramatically

Our Strategy – Improve Performance

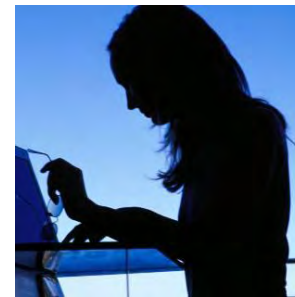
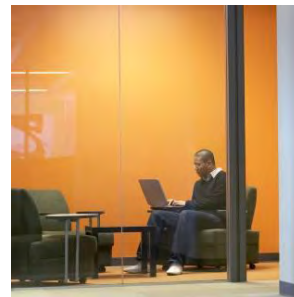
- **Risk Office Enhancements**

- Expanded hours of availability (hours are now 8am-11pm ET M-F continental US business hours)
- Expanded services (subscription hours are now up to 120 hours)
- Monthly WebEx for clients
- Increased staffing

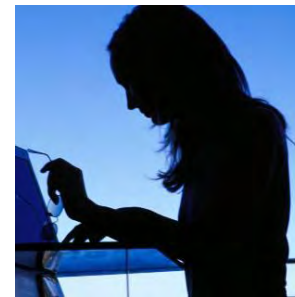
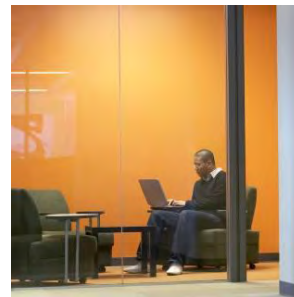
- **Integrated Transaction Rules Engine**

- Enables Fiserv or the Financial Institution to create rules designed to stop fraud and monitor rule performance
- Fraud mitigation will start when the rule is triggered
- Allows a more robust and complex set of authorization decision rule sets for both debit and credit

Footnote (Arial 8pt)



Panel Discussion



Thank you!

JB Rambaud
jb.rambaud@fiserv.com
(503) 796-6487