



# Workshop on Cybercrime Legislation

Bogotá, Colombia  
September 3-5, 2008





# Cybercrime Legislation Workshop

- Goals
  - Understand a legal framework against cybercrime
  - Recognize good practices regarding cybercrime law
  - Identify steps towards strengthening cybercrime law
- Country cybercrime legislation profiles
- Program



# Cybercrime Legislation Workshop

- Participant introductions
  - Name, country, organization
  - Role in developing cybercrime legislation
  
- Moderator introductions



# Cybercrime and Electronic Evidence

Michelle Kane and Albert Rees  
United States Department of Justice  
Computer Crime and Intellectual Property Section



# The Cybercrime Threat

## Electronic Evidence is Everywhere

## Legislation to Address the Threat



# The Cybercrime Threat

Electronic Evidence is Everywhere

Legislation to Address the Threat



# What is "Cybercrime"?

- Offenses against computer data and systems
- Offenses related to computers and the Internet

**Computers are essential to the crime.**



# Offenses Against Computer Data and Systems

- **Illegal interception**
  - Interception of data to, from, or within a system
- **Illegal access**
  - May compromise data or confidentiality
- **Data interference**
  - Damaging, deleting, deteriorating, altering, suppressing
- **System interference**
  - Seriously hindering the functioning of a system
- **Misuse of devices**
  - Access devices, computer passwords





# Offenses Related to Computers and the Internet

- Computer-related forgery
  - With intent that it be acted upon as if it were authentic
- Computer-related fraud
  - Interference with system or data with intent to defraud
- Child pornography
  - Producing, offering, distributing, procuring, possessing
- Intellectual property infringement
  - Willful infringement on a commercial scale



# Globalization of Cybercrime

- Cybercrime by its nature easily crosses borders
- Enables worldwide organization of profitable criminal activity
  - Identity theft
  - Sale of hacking tools
  - Creation of custom malware
  - Renting botnets
  - Spamming operations
  - Money laundering
  - Intellectual property infringement
- Involvement of transnational organized crime and terrorist groups

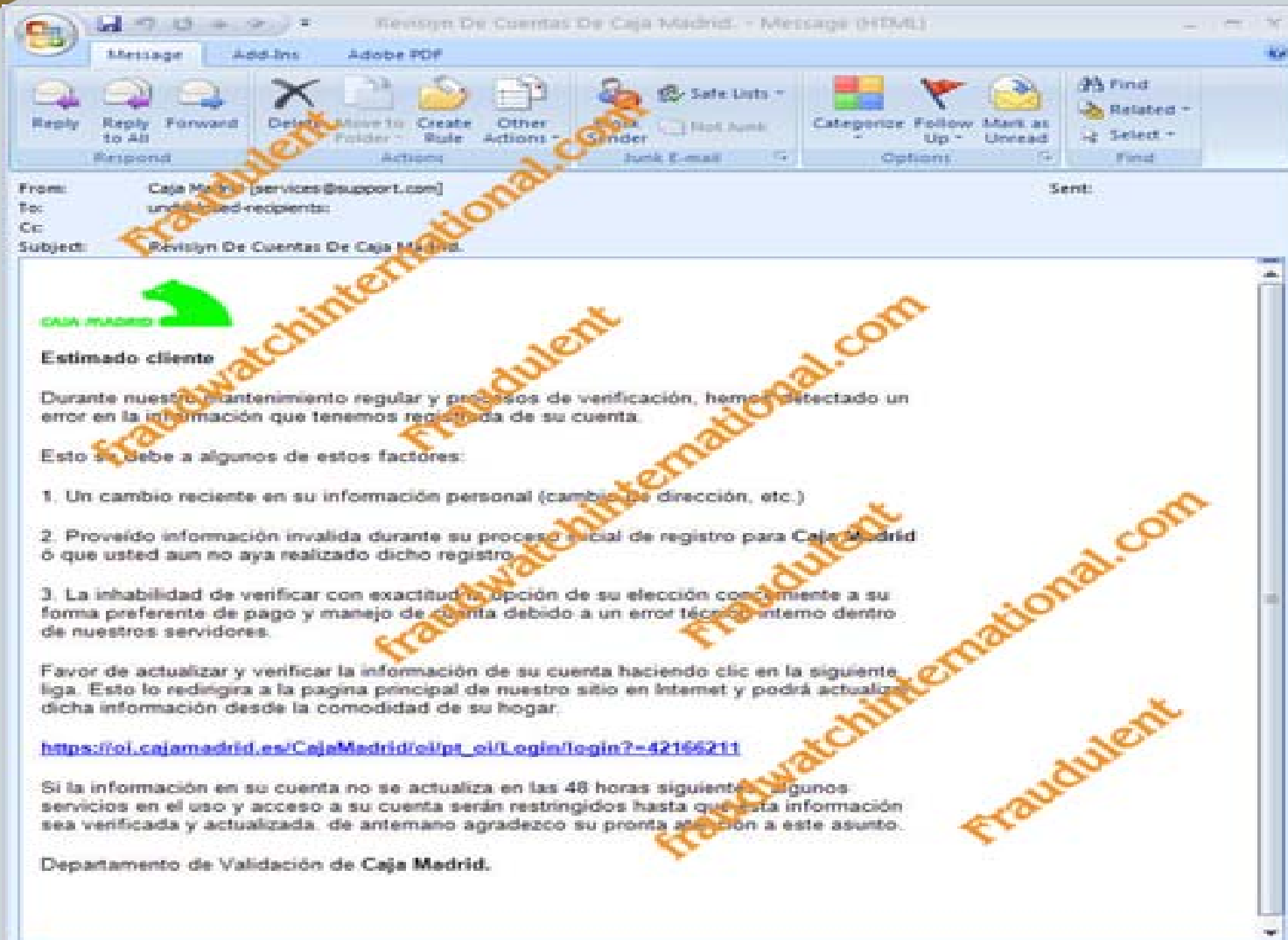


## Example: Phishing

- A type of “social engineering” characterized by the attempt to fraudulently obtain confidential information (computer-related fraud)
- Anti-Phishing Working Group Statistics (January 2008):
  - **20,305** unique phishing websites reported
  - **29,284** unique phishing reports received
  - **131** brands “hijacked”
  - Most targeted industry sector: **Financial services** (92.4% of all attacks)
  - Principal countries hosting phishing sites:
    - #1: United States (37.25 percent)
    - #2: Russian Federation (11.66 percent)
    - #3: China (10.3 percent)



# Caja Madrid – June 2008



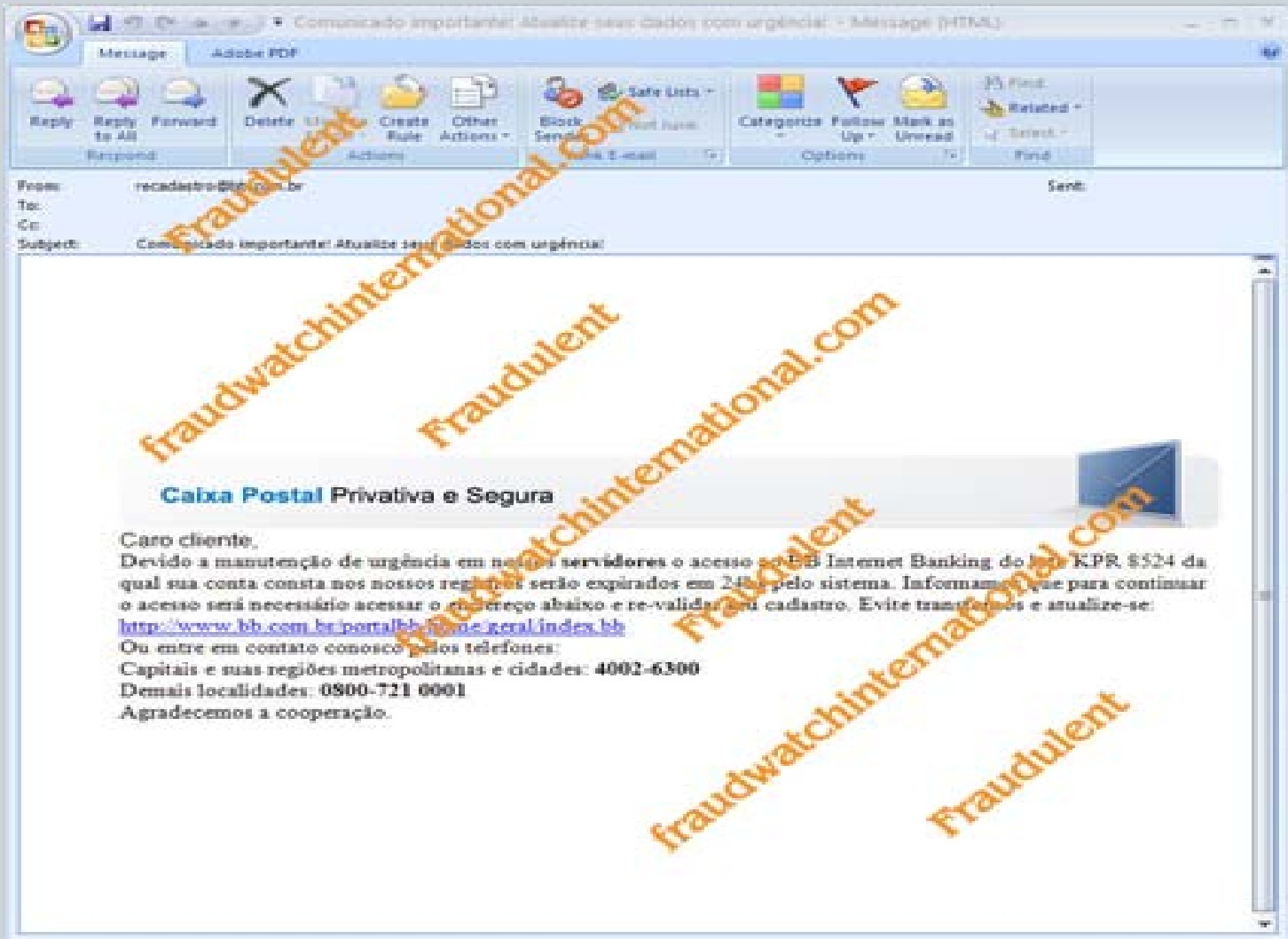


# Caja Madrid – June 2008





# Banco do Brasil – July 2008





# Banco do Brasil – June 2008





## Example: Carding Forums

- Phishing or hacking (illegal interception, illegal access, misuse of devices) to obtain personal identity information
- Online activity (computer-related fraud) to buy, sell, and use the stolen identities
- From stealing the information to cashing out, the operation spans the globe





# Sale of Stolen Credit Card Data

International Carder's Alliance :: View topic – ёОУОфлЮ ОАО%†, %о†Ю°  
URL: http://forum.carderplanet.net/viewtopic.php?t=2924

Author	Message
<b>Gabrik</b> Capo di Capi  Joined: 31 Mar 2002 № 2272 Posts: 60	<p>■ Posted: Fri Apr 12, 2002 8:56 pm Post subject: Постоянно продаю Visa/MC европа и штаты!!!</p> <p><b>Постоянно продаю дампы TRACK 2 в наличии всегда есть USA&amp;EURO!</b> <b>Дампы с экспиром текущего месяца продаются всего за 5\$</b> Внимание проверка дампа на валидность непосредственно перед прокаткой тоесть перед входом в банк или шоп вы заходите в интернет стучите мне на асю и кидаете карты через 2-3 мин я даю ответ по ним и вы спокойно шопитесь по рабочим картам, что очень удобно при прокатке второй и третий раз что бы не на авось а точно зная что всё ок. Подробности читайте <a href="#">здесь</a> Так же можно купить не проверенные дампы USA по 10 грн штука. Валид 70-80% без замены. Тоесть проверяете сами. Перед продажей дампы проверяются в европе на работоспособность и после проверки живёт долго что проверено экспериментами неоднократно, соответственно продаются штатовские дампы только работающие в европе а не закрытые на локалку только для штатов. Так же я сделаю выборку по бину ,банку ,стране и Внимание новый сервис продажа дампов Gold&amp;Pl Цена Gold&amp;Platinum USA = 90\$ Europa Gold&amp;Platinum = 110\$ Оплата по WM. USA от 1 до 20 штук -30\$ от 20 до 50 штук -25\$ от 50 до 100 штук -20\$ свыше 100 обговаривается отдельно  Европа от 1 до 20 штук -40\$</p>

Gabrik: “ Always in stock dumps from Track 2, USA & Europe ”

“ Dumps available in selections sorted by BIN, by bank, by country, or by dump's final digits. New service: Gold&Platinum dumps!!! Price: Gold&Platinum USA = \$90 Gold&Platinum Europe = \$110 ”



# Counterfeit Licenses and Credit Cards

ASAD's Team - Index - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop  Search



English

[Главная](#) | [Вод. права](#) | [Платёжные карты](#) | [ЧаВо](#) | [Связь](#)

*Добро пожаловать,  
Предлагаем Вашему вниманию самые качественные платёжные карты и вод. удостоверения.*

Driver Licenses	Payment Cards
	

Copyright © 2003 by the ASAD's Team. All rights reserved.

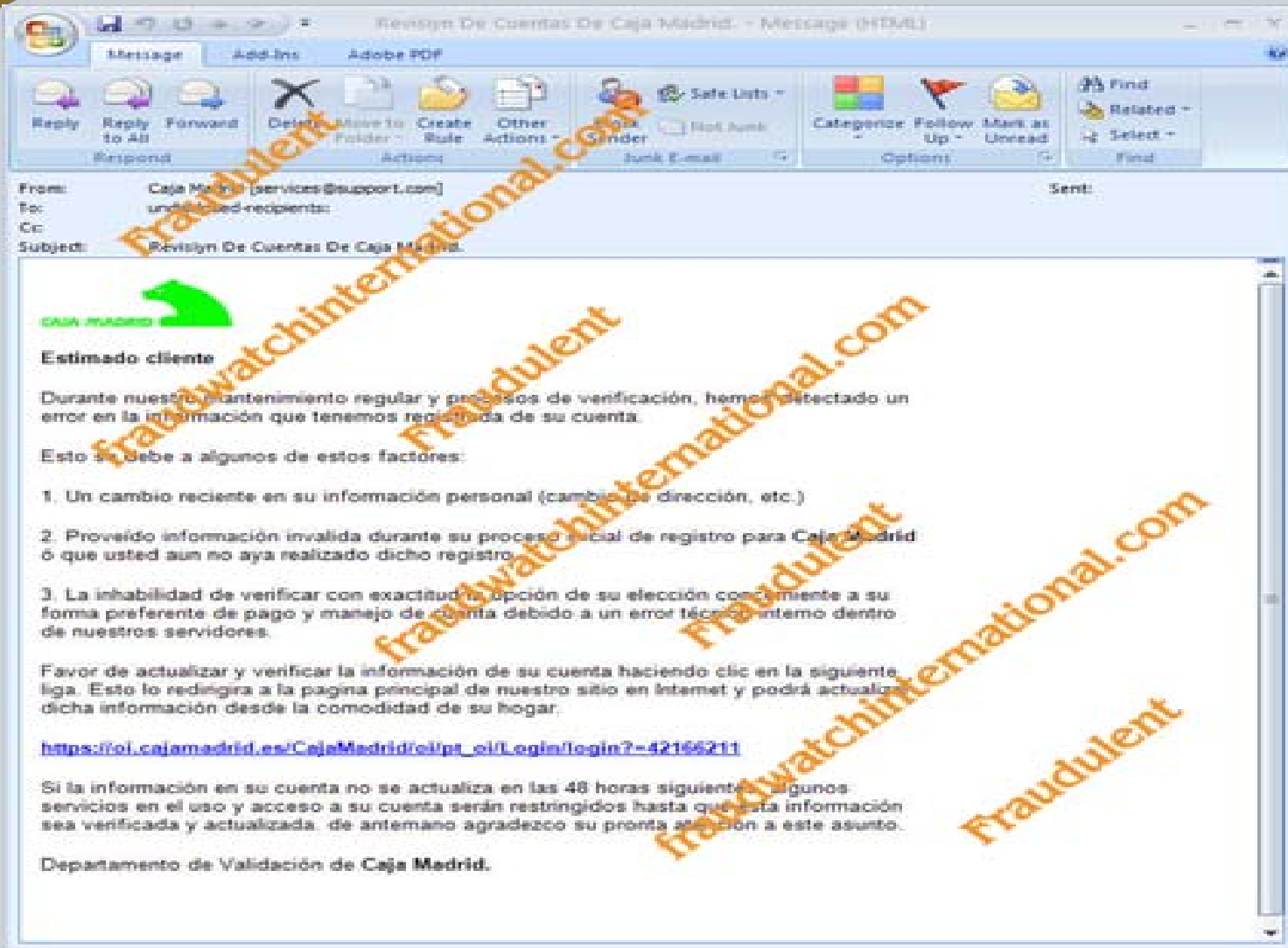


## Example: Phishing

- A type of “social engineering” characterized by the attempt to fraudulently obtain confidential information
  
- Anti-Phishing Working Group Statistics (January 2008):
  - **20,305** unique phishing websites reported
  - **29,284** unique phishing reports received
  - **131** brands “hijacked”
  - Most targeted industry sector: **Financial services** (92.4% of all attacks)



# Caja Madrid – June 2008



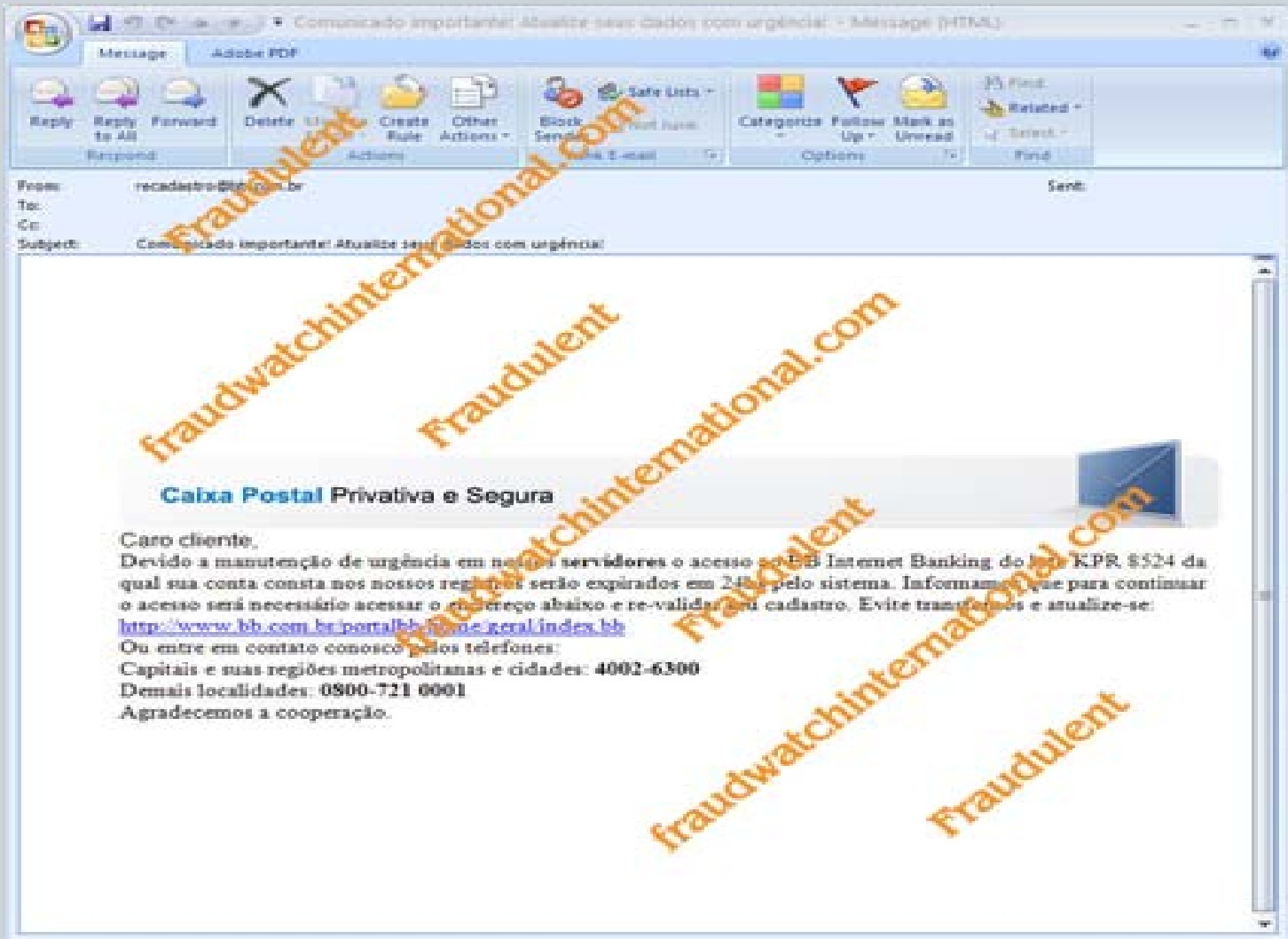


# Caja Madrid – June 2008





# Banco do Brasil – July 2008







# Banco do Brasil – June 2008





# Snapshots of Global Cybercrime

- Over 5 million bot-infected computers and over 4,000 bot command-and control servers identified in six months\*
- Over US\$1.5 million traded on one carding channel in one day. \*\*
  - Credit cards sold for between US\$0.40 and US\$20\*
  - Bank accounts can be cashed out in 15 minutes\*
- Data breach cost per incident was US\$6.3 million\*
- Almost 400,000 new malicious code threats in six months\*

\*\*Source: Team Cymru

\*Source: Symantec Global Internet Security Threat Report, July-December 2007





## The Cybercrime Threat

Electronic Evidence is Everywhere

Legislation to Address the Threat



# Crimes Create Electronic Evidence

- Any crime can create electronic evidence
- Computer to commit crime
  - Illegal access to computer systems
  - Interference with data or computer systems
  - Online identity theft



# Crimes Create Electronic Evidence

- Computer to store evidence of crime
  - Child pornography photographs
  - Pirated movies and other intellectual property
  - Records of criminal transactions
  
- Computer for communication
  - E-mail
  - Voice and video communications
  - Transfer documents and photographs



# Computers Create Records

- Computers create transaction logs
- Electronic documents, images, and other files contain hidden (and helpful) information

**Most criminals do not know about  
the electronic evidence they create!**



# DIGITAL STORAGE DEVICES





# Digital Storage Devices

- CD, DVD, and other disks
- Thumb drives, flash drives
- Personal digital assistants (PDA)
- Digital cameras
- Printers, fax machines



- Mobile phones
- Media players – iPod, MP3
- Game consoles – PlayStation, Xbox
- Automobiles? – OnStar, GPS





# Networks and the Internet

- Computers rarely stand alone



- Networks – local, area, wireless
- The Internet

All electronic information is at a  
**physical** location.



# Service Providers and Infrastructure

- Internet infrastructure relies on service providers



- Service providers control important electronic evidence
  - Electronic communications
  - Stored data
  - Customer information





# Data Is Volatile

- Deleted by a keystroke
- Deleted in normal course of business
- Lost when computer turned off
- Specialized knowledge and tools needed to recover deleted data
- Some data cannot be recovered

**Investigators must act quickly  
to preserve electronic evidence.**



The Cybercrime Threat

Electronic Evidence is Everywhere

Legislation to Address the Threat



# Addressing Cybercrime

- New technologies challenge existing legal concepts
- Computer networks are international – they ignore jurisdictional boundaries
  - Intentional criminal conduct across borders
  - Unintentional effects of criminal conduct
- Domestic legislation is the primary means for addressing cybercrime and electronic evidence issues



# QUESTIONS?

The Cybercrime Threat

Electronic Evidence is Everywhere

Legislation to Address the Threat



michelle.kane@usdoj.gov | albert.rees@usdoj.gov

+1 (202) 514-1026

