Misuse of Open Loop Prepaid Cards

David Murray (david.murray@do.treas.gov)
U.S. Treasury Department
Office of Terrorist Financing and Financial Crimes

Evolving Safeguards

- Initially, few safeguards
  - Easy to find anonymous, high value limit products.

- Now, more safeguards in place
  - 2007: OTS said its banks “should develop systems to apply the customer identification program” to open system reloadable prepaid cards.
  - Program managers have compliance departments, monitor transactions and file SARs.

Evolving Criminal Use

- Initially, the crimes had some nexus to the Internet
  - Bank fraud and identity theft.
  - Online drug sales.
  - Online gambling.

- Now, seeing cards used in other types of crime
  - Embezzlement.
  - Hand-to-hand drug sales.
  - But information being generated is now more useful to law enforcement.

Milad Ghattan (2006)

- Milad Ghattan purchased stolen credit card numbers online.
- Used the stolen credit card information to purchase “Virtual Visa” prepaid cards.
- Used the cards to obtain funds in three ways.

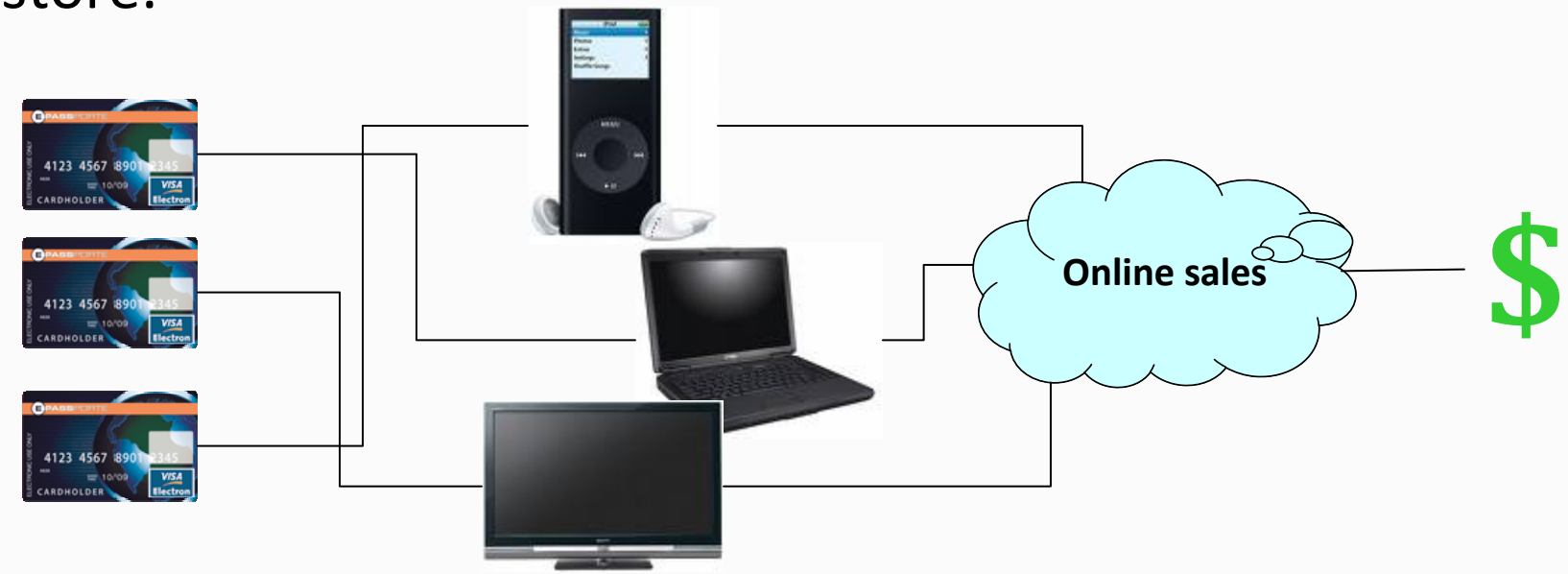
Milad Ghattan (2006)

- 1. Milad used the Virtual Visa cards to pay his tuition at the University of North Carolina at Greensboro.

- Milad overpaid his tuition by $31,000 and asked UNCG to issue him a check for the balance.

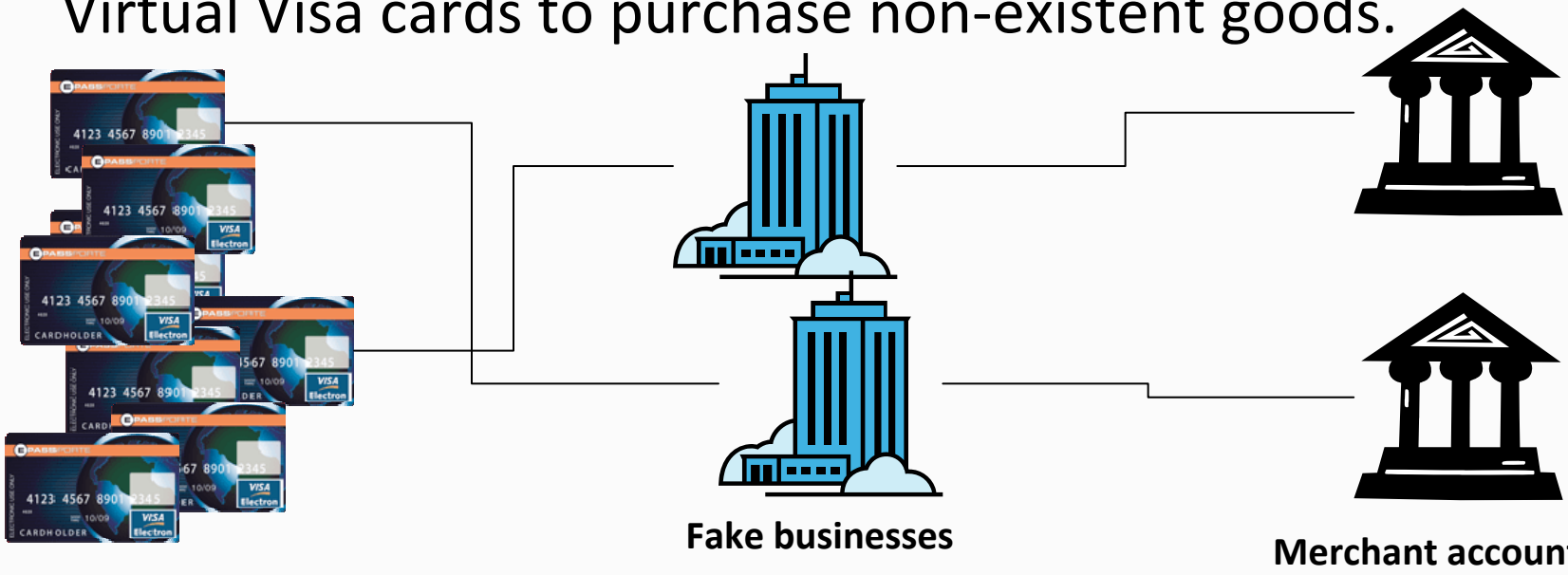
Milad Ghattan (2006)

- 2. Milad also purchased goods online using the Virtual Visa cards and had them shipped to his brother's auto parts store.



Milad Ghattan (2006)

- 3. Milad established obtained credit card merchant accounts for fictitious online businesses and used the Virtual Visa cards to purchase non-existent goods.



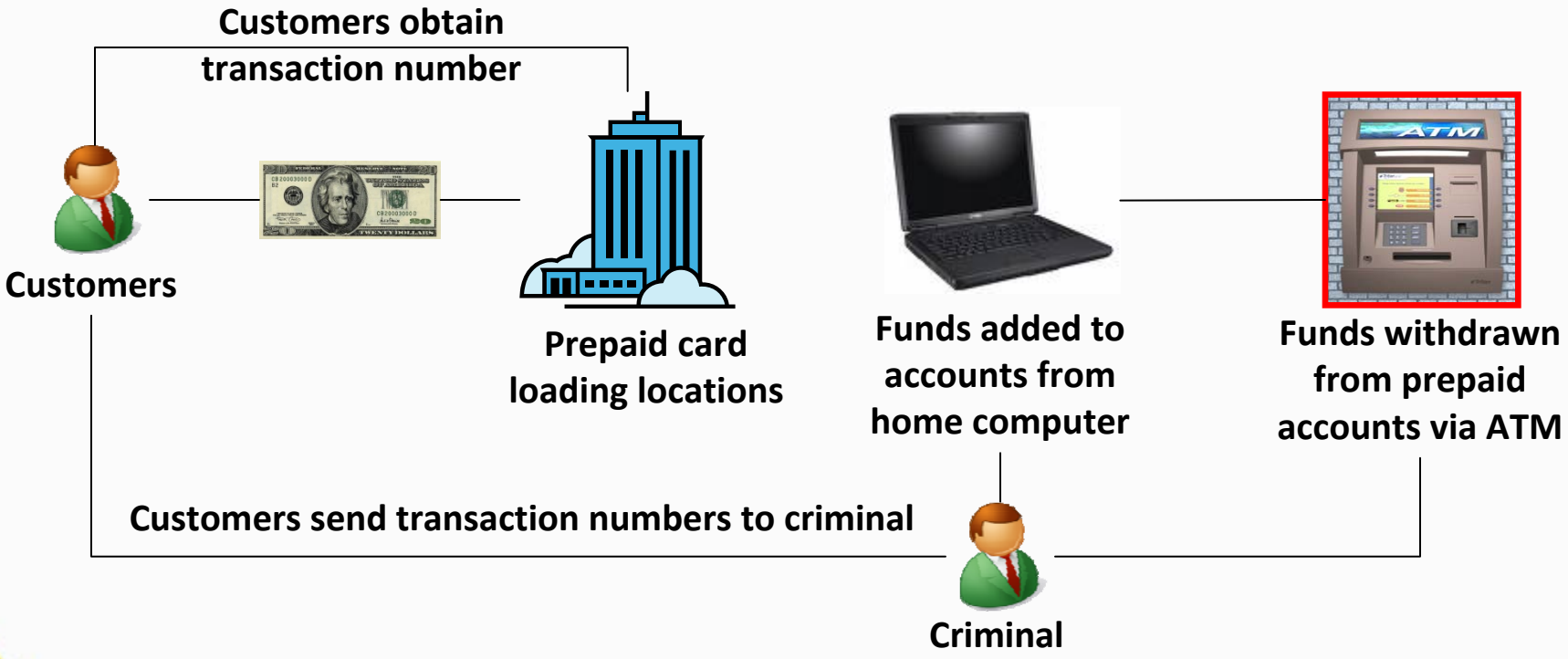
- In all, he stole at least $90,000 in 15 months.

Israel Sanchez (2007)

- Sanchez sold steroids online.
- Initially, he had customers send him money via a money transmitter.
- Later, he decided that receiving funds via a prepaid card network would be easier and more anonymous.
- Sanchez had 10 prepaid card accounts, all of which he established using aliases.

Israel Sanchez (2007)

- Sanchez told customers to send him money via a prepaid card company's network. He withdrew funds from ATMs.

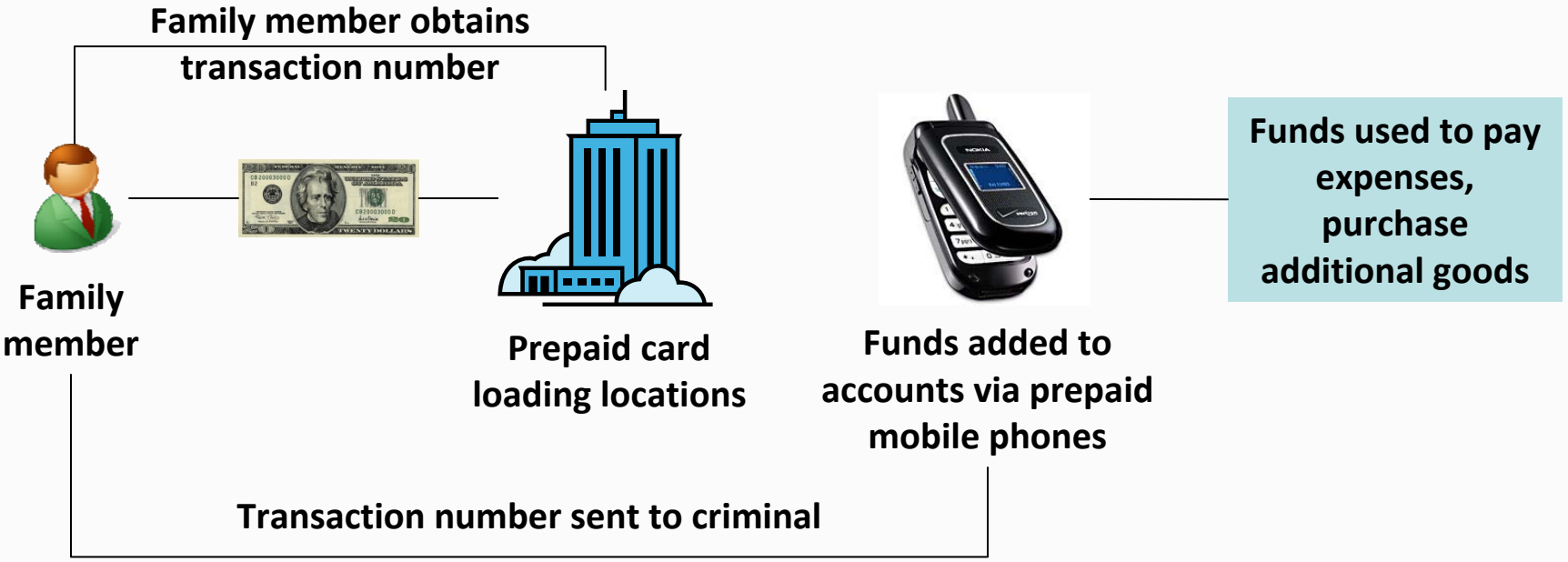


BGF (2009)

- The Black Guerilla Family (BGF) is a nationwide prison gang.
- The BGF smuggles narcotics and other contraband into prisons. In May, one member was convicted of murder.
- Before a series of arrests in early 2009, the BGF was attempting to take over the drug trade in Maryland prisons and had been expanding its footprint in Baltimore's violent narcotics trade.
- The BGF had numerous reloadable prepaid accounts, all of which appear to have been established by real people.

BGF (2009)

- The defendants instructed their customers – mostly prisoners – to pay the gang by having family members transmit money through a prepaid card network.

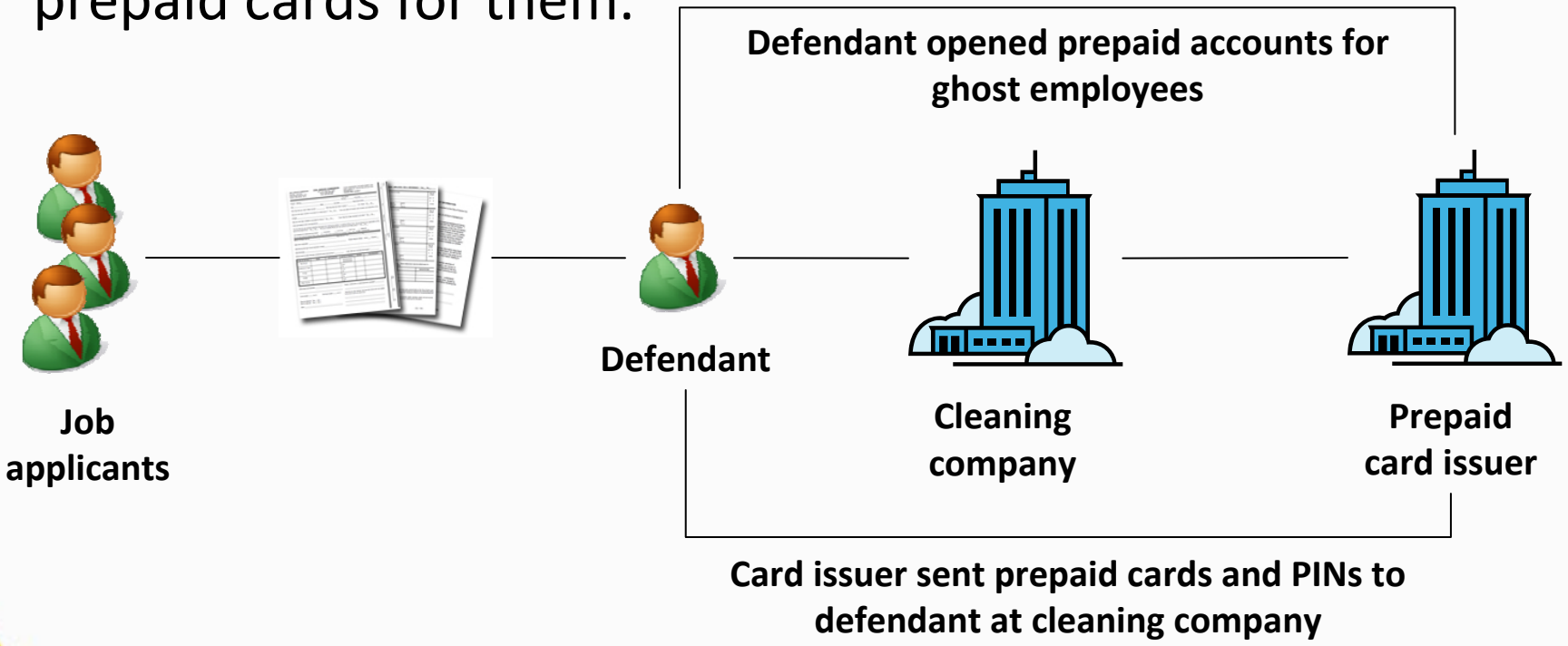


Jose Rosado (2009)

- Jose Rosado worked for a cleaning company that had a contract with George Mason University.
- The cleaning company paid its unbanked employees by depositing funds into prepaid card accounts.
- Rosado is accused of hiring ghost employees and establishing prepaid card accounts for the ghost employees.

Jose Rosado (2009)

- Rosado allegedly put job applicants on the payroll without telling them they had been hired. He also obtained prepaid cards for them.



Jose Rosado (2009)

- This use of ghost employees to embezzle funds is common, but the use of prepaid cards was novel.
- Paper checks would have made the scheme more complex:
  - Defendant would have had to find a check casher willing to be complicit in laundering funds, or
  - Defendant would have had to recruit people willing to serve as ghost employees and cash the checks.
- As prepaid payroll cards become more common, so will this method of laundering funds.

Prepaid Card Controls

- Manage risk by:
  - Verifying customer identification and
  - Ensuring transaction monitoring and recordkeeping.

- Reduce chances of one person circumventing transaction and value limits by:
  - Matching data other than name (i.e. address, phone number) and
  - Monitoring transactions for patterns that suggest one person has more than one account.

THE FUTURE

The Future

- Moving away from face-to-face transactions.
  - Today, it's a card. Tomorrow, it could be a phone.
  - Tower Group predicts that mobile banking in the United States will **grow at a rate of 51.9 percent** between now and 2013.
  - Puts greater importance on back-end transaction monitoring.
  - Weak back-end monitoring increases fraud exposure.

- As licit commerce increasingly flows through your channels, illicit activity will also increase.

RBS WorldPay

- RBS WorldPay – U.S. payment processing arm of The Royal Bank of Scotland – announced in Dec ’08 that its systems had been hacked.
  - 1.5 million prepaid cardholders’ info stolen.
  - Withdrawal limits reset on ~100 payroll cards.
- 130+ ATMs in 49 cities from Moscow to Atlanta hit simultaneously just after midnight ET on Nov 8, ’08 resulting in ~$9 million withdrawn.

Laundering Using ATMs

Luis Saavedra

- ATM misuse well documented.
- Saavedra plead guilty in 2007 in NY to money laundering
- He and a partner are believed to have used family, friends, and hired hands to open 380 bank accounts in 6 states
  - Saavedra routinely made deposits of $500 to $1500 in each account – *microstructuring*
- Sent ATM cards to Columbian drug cartel to access the cash
- Number of ATMs in Colombia more than doubled between 1995 and 2000, rising from 2,238 to 5,520, according to the Banking Association of Colombia.

Illicit ATM Use Well Established

- First FinCEN SAR Bulletin (June '99)
  - 982 SARs (June '97 to mid-April '99) cited ATM activity in the narrative.
    - 30% involved cash or wires from outside the United States deposited in U.S. accounts and then withdrawn via ATMs outside the U.S.
- 9,000 SARs filed from 2003-2007 referencing prepaid or stored value cards

Terrorist Financing

- Jakarta terrorists using straw account holders to establish accounts and conceal their identities.
- Reinforces the importance of monitoring transactions for patterns that suggest the named account holder is not controlling the account, or that someone other than named account holders are controlling multiple accounts.

Conclusion

- Value limits and transaction limits are not effective deterrents when criminals can circumvent those limits by establishing multiple relationships.
- Criminal use of prepaid cards is migrating from Internet-related activity to other types of activity.
- The trend away from face-to-face transactions makes back-end transaction monitoring more important.
- Criminals are exploiting prepaid card and ATM networks to steal money from financial institutions.