# CS 523: Social, Economic, and Legal Aspects of Security

## Disputed Transactions

# Disputed transactions

- A business says to a customer: “you did X and must pay the $200 that it costs”
- Customer says “I did not do X, I will not pay”
- What happens when neither can provide conclusive evidence? Which one loses $200?
  - Such disputes are frequent with new technologies
  - Answer depends on where the law places the burden of proof (on customer, or on business?)

# Case study: ATM fraud

- Phantom withdrawals
  - When bank says customer withdrew $200 in cash from at an ATM machine, but customer denies it
- Which of them is going to lose $200?
  - Banks claimed their systems were infallible, that the records from their systems were proof enough ("otherwise what would stop customers from massively withdrawing cash then denying it?")
  - Many countries bought banks' argument

# U.S. placed burden on banks

- Dorothy Judd v. Citicorp (1980)
- Judd denied she made the cash withdrawals, Citicorp insisted she must have made them
- Judge ruled in favor of Judd
  - Against bank's claim to an infallible system
  - Against placing burden of proof on Judd
- Federal regulations were modified accordingly
  - Burden of proof is on banks, not on customers

# In many countries, burden on customer

- Most European countries (UK, Germany, Italy, Netherlands, Norway, …)
- Whenever a customer contested a cash withdrawal, the bank sued the customer
  - "Our systems are secure, so the customer must be trying to defraud us" − the courts believed them
- Resulted in egregious miscarriages of justice
  - Customer victims included police workers like John Munden (1992), Jane Badger (2008)

# Placing burden on customer (cont'd)

- Such countries suffered much more ATM fraud than in the U.S. (for some, epidemic)
  - Not what the banks predicted
- Most fraud was the banks' fault
- Bank sloppiness in their operations, e.g.,
  - In mailing cards and PINs (easy to intercept)
  - In giving replacement to a "forgotten" PIN (insufficient verification of identity)

# Placing burden on customer (cont'd)

- Massive theft by bank staff
  - They know the system, and they know there will be no serious investigation (the customer will be blamed and will have no recourse)
- Banks deployed flawed technology
  - The very one they were claiming to be infallible
- Banks did not deploy effective technologies
  - Banks that deployed ATM cameras were pressured by other banks into withdrawing them

# One of the “infallible” bank systems

- Card issued to customer had 2 separate fields
  - One magnetic strip for the account number
  - The other magnetic strip contained the PIN encrypted using the bank’s secret key (same secret key is in a secure processor within the ATM machines)
- Andrew Stone’s observation: Can replace first field with someone else’s account number and withdraw money from their account
  - He and others did, massively until exposed (customers’ class action lawsuit failed to get their money back)

# Meanwhile, in the U.S.

- Losses from customer misrepresentations were tiny (unlike what banks had predicted)
  - They're about 1/3 of losses to physical vandalism
- Losses from non-customer fraud were much lower than in the UK, even though security spending by U.S. banks was much lower
  - Why was the security-related money spent more effectively by U.S. banks? Probably because they faced a fierce liability regime (powerful incentive)

# Case study: Bank account theft

- Alice wakes up, checks her bank account, and finds out that it was emptied overnight through multiple transactions that she never authorized
  - She calls her bank and, after 45 minutes of listening to awful music and recorded messages, gets a human from whom she learns that the withdrawals were to pay for the credit card bills of a certain "Bob"
- Info that Bob (or "Bob") needed to carry this out:
  - The bank's routing number (public, on bank web site)
  - Alice's account number (printed on Alice's checks)

# How Bob generated each transaction

- Bob connected to his credit card's web site
- Bob clicked "Pay My Bill"
- As source of the funds to pay his bill, Bob entered Alice's banking information
- That's it ! The credit card company took the money out of Alice's bank account
  - Neither the credit card company, nor Alice's bank, ever contacted Alice to ask for her approval

# How did Bob get Alice's bank info?

- He could have bought it from the illegal markets for such info
- How do the illegal markets get the info?
  - From corrupt bank employees
  - From people who handle physical checks (landlords who get paid by check, employees of utilities whose customers pay by check, … etc)
  - From break-ins at companies, that reveal banking info of employees on the company's payroll

# Likely consequences for Alice

- No loss of money *if* she *promptly* catches and reports the fraud
  - Her bank would work with the credit card company to reverse the transactions
  - Note that someone who does not balance their checkbook may not notice a small-amount fraud (so a clever Bob would not have emptied Alice's account, he would have taken a tiny slice from it)
- She has to close bank account, open new one

# How to self-protect

- Do not write any paper checks, to anyone
  - Even to someone you trust, because processing the check takes it through too many hands
  - The rent check you use to pay your landlord is also seen by her accountant, the courier who drives and delivers it to the bank, bank employees
- Do not use your bank account for auto-pay of monthly bills (utilities, subscriptions, etc)
  - Use your credit card instead (loss limited to $50)

# How to self-protect (cont'd)

- Do not keep large balances in the bank account whose info you shared, e.g.,
  - You wrote checks drawn on the account
  - You provided the account number to entities that pay you (as employee or consultant) – the info you provide for the purpose of putting money *into* your account can be used to get money *out of* it
- Move the money promptly to another account
  - OK if it is at the same bank