

Fraud-Proofing your Credit Union: Online Banking Fraud

May 6th, 2008





Overview

- **Online banking fraud attacks**
- **Strategies for fighting back**
- **Case study:**
 - Interac Email Money Transfer (IEMT)
- **Summary**



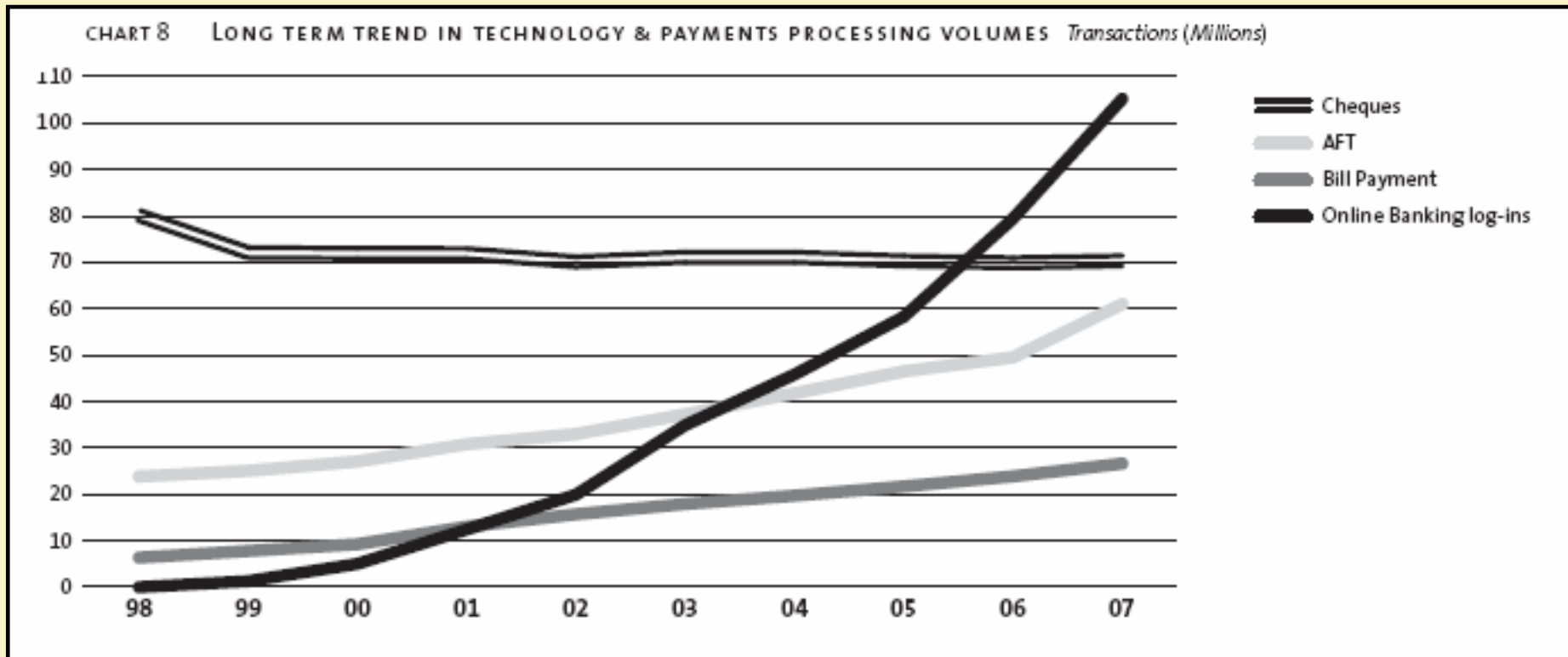
Overview

- **Online banking fraud attacks**
- Strategies for fighting back
- **Case study:**
 - Interac Email Money Transfer (IEMT)
- Summary



Growth in Online Banking (CUCBC)

- **32.5% increase in Member logins (2006-2007)**
- **~ 105 MM online banking transactions in 2007**



Source: CUCBC 2007 Annual Report



The Basics: Getting into the mind of a fraudster

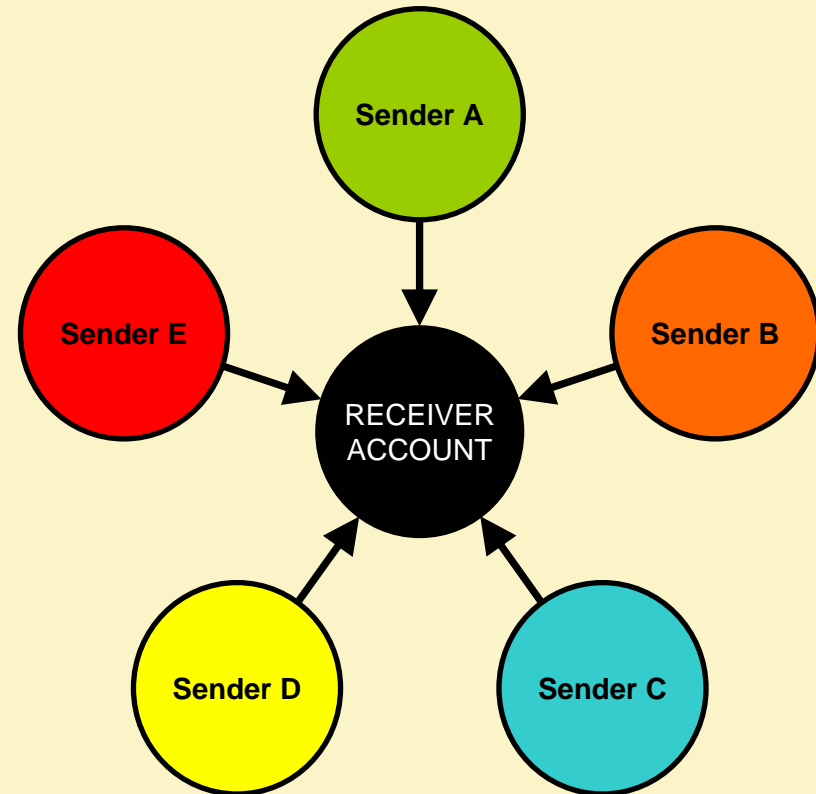
- **Why exploit online banking?**
 - Easy of exploitation (static passwords)
 - Speed of exploitation
 - Information sharing between FI's is restricted
 - Lower risk
 - International





What do fraudsters need to commit online banking fraud?

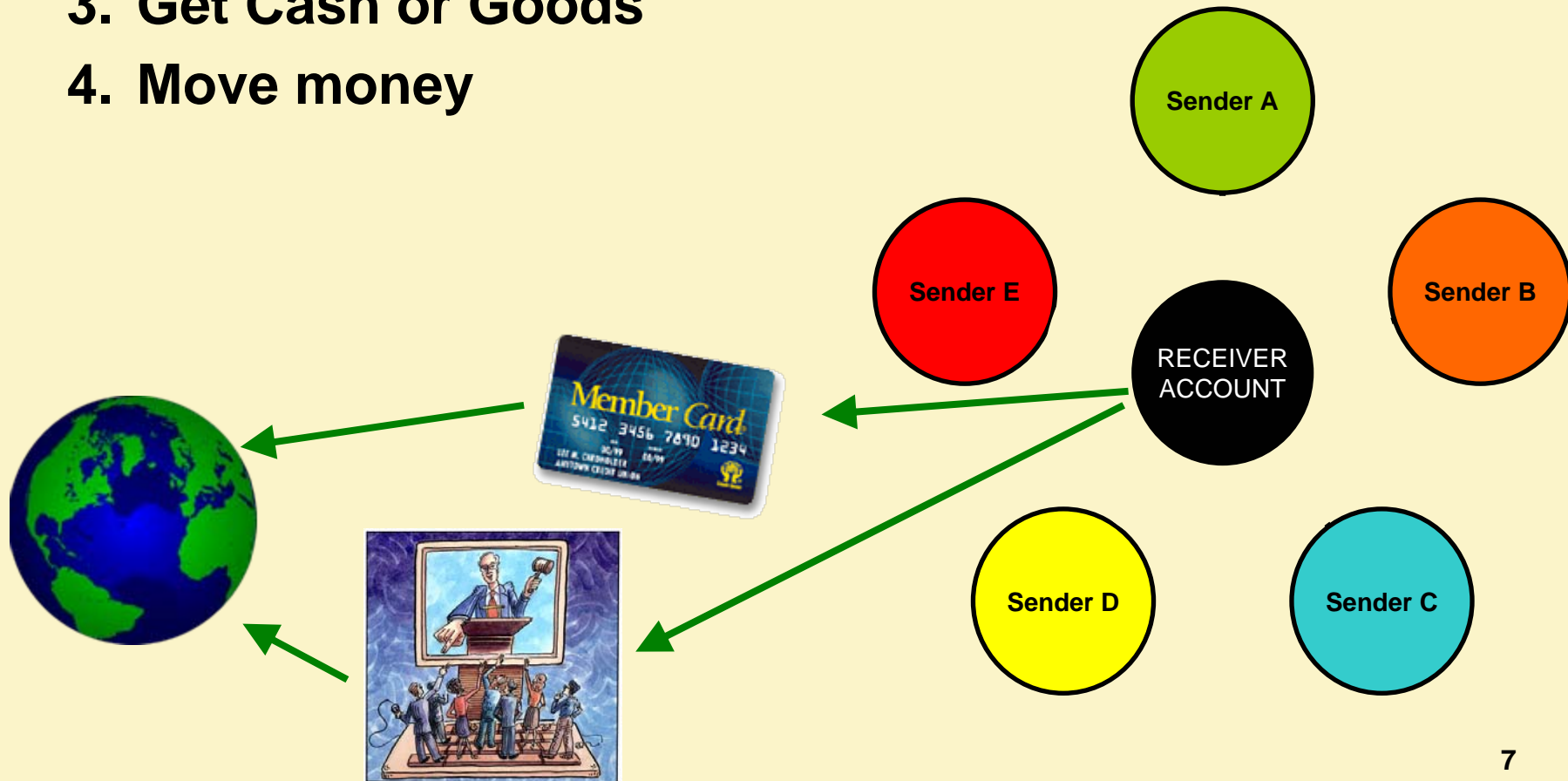
- **Web banking credentials**
 - Traditional account takeover
 - Phishing / Spear-phishing
 - Technical subterfuge
- **Receiving account**
 - Fake account opening
 - Job Recruitment
 - Purchase Goods online





How it works?

1. Get access to Sending Account
2. Get access to Receiving Account
3. Get Cash or Goods
4. Move money





Overview

- Online banking fraud attacks
- **Strategies for fighting back**
- Case study:
 - Interac Email Money Transfer (IEMT)
- Summary

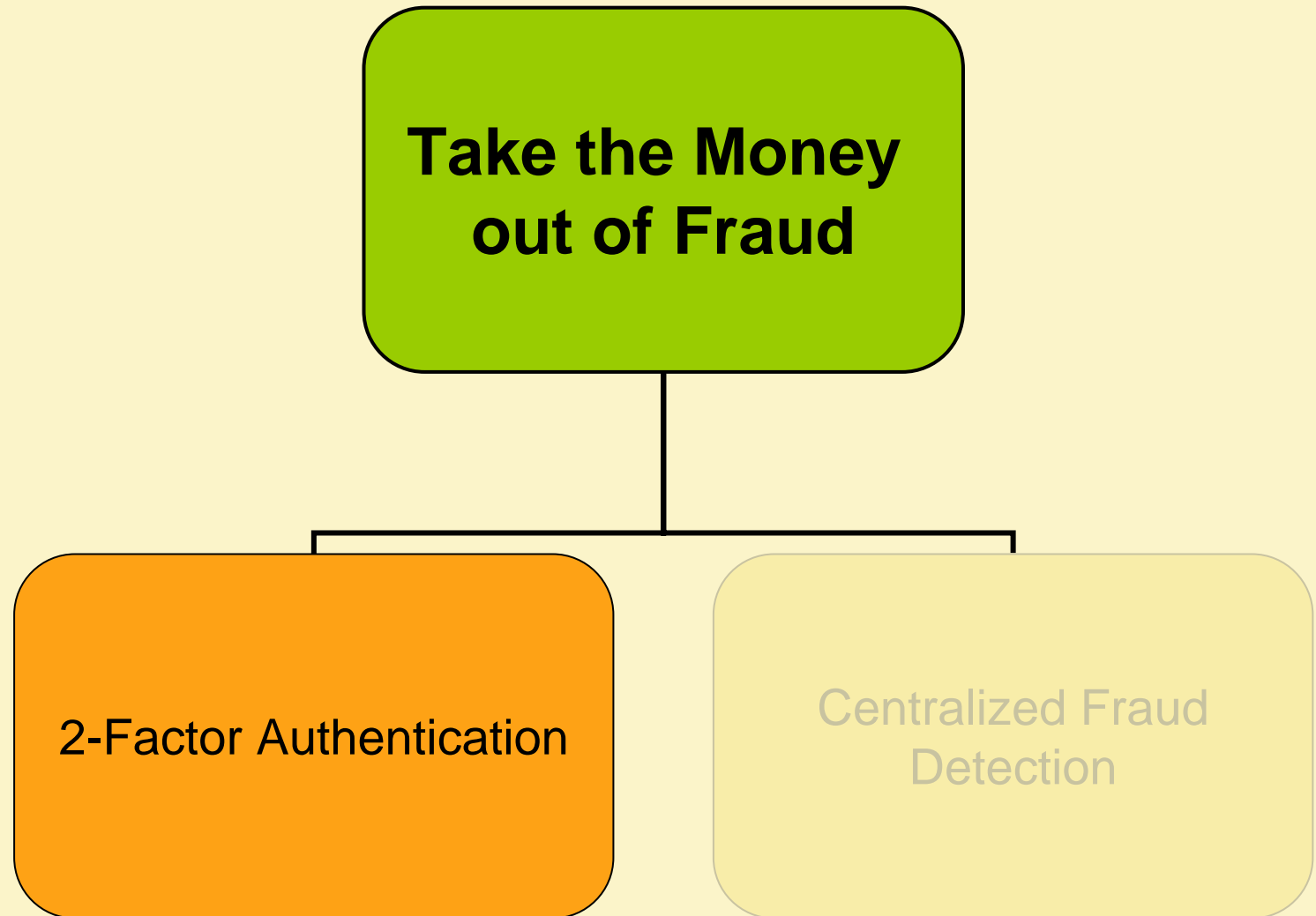


Protecting web banking credentials

- **Difficult to do with static password authentication**
- **Fighting Phishing:**
 - Customer education
 - Leveraging ISPs
 - Pay Pal White Paper (April 2008)
- **Fighting technical subterfuge**
 - Client virus and spyware protection
 - Customer education



Fraud Management Strategy





Protecting web banking credentials

The single most effective proprietary strategy is 2-Factor Authentication

Something you know...

- Static
- Password / PIN



AND...



....something you have:

- Dynamic
- One time

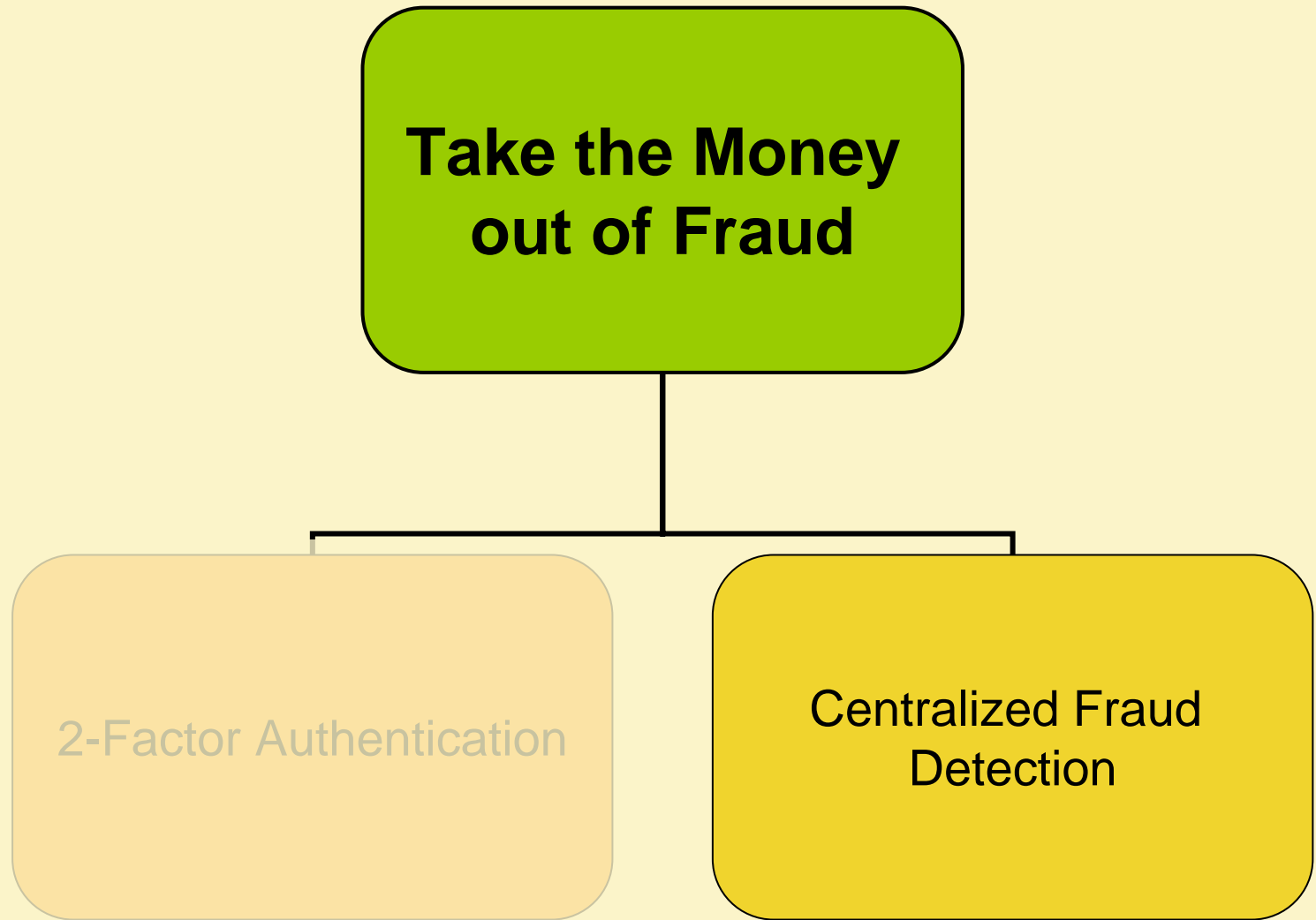


The “Something you have”:

- **Tokens**
 - RSA one-time password generators
- **Online chip card readers**
 - Plug into your computer and use with chip card
- **Offline chip card readers**
 - Chip Authentication Protocol (CAP)
- **Mobile phones with SMS**
 - Sends one-time password
- **USB devices**
 - Plug into computer with encrypted information from Issuer
- **Scratch Cards, Printed “Bingo” Cards**
 - Issuer asks for a letter/number combination on reference card



Fraud Management Strategy





Overview

- Online banking fraud attacks
- Strategies for fighting back
- **Case study:**
 - Interac Email Money Transfer (IEMT)
- Summary



INTERAC Email Money Transfer (IEMT)

How it works

- **The Sender:**

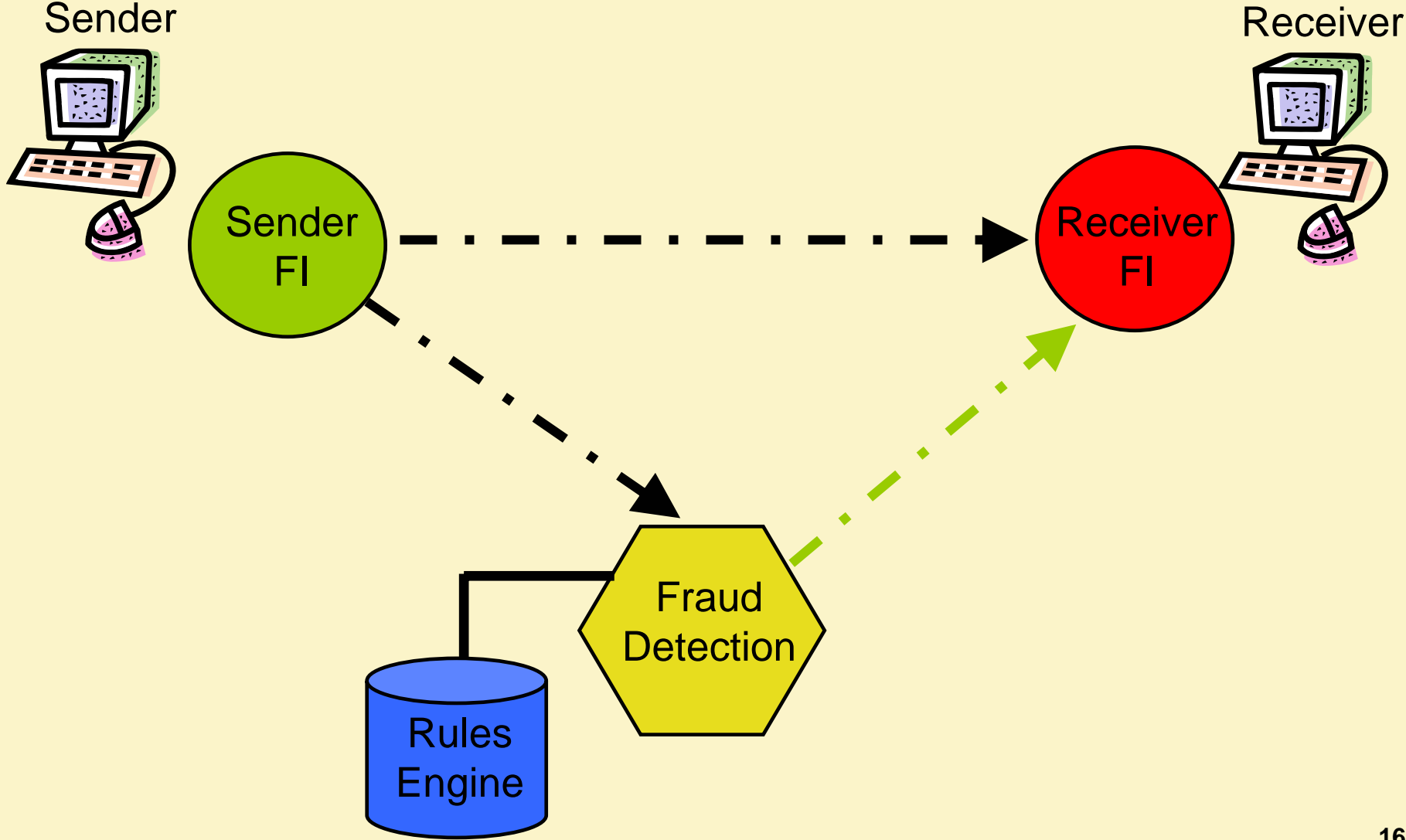
- Logs into web banking
- Choose to transfer funds
- Selects IEMT
- Enters recipient email address and selects a security question
- Confirms the transfer amount

- **The Recipient:**

- Received email with link to IEMT home page
- Selects their Financial Institution
- Logs into web banking
- Answers the security question
- Receives funds



Centralized Fraud Detection





Benefits of Centralized Fraud Detection

- **Detect fraud based on industry patterns**
- **System learns in real-time**
- **Fraudsters exploit FI's having to play by rules**
- **All transactions and fraud is reported**
 - Everyone benefits from single FI's learnings
- **Cost savings**
- **Flexibility**



Hold for Fraud Losses to Total Volume



Overview

- Online banking fraud attacks
- Strategies for fighting back
- Case study:
 - Interac Email Money Transfer (IEMT)
- **Summary**



Summary

- **Online banking fraud attacks are increasing**
- **Take the money out of fraud**
 - 2-Factor Authentication
 - Centralized Fraud Detection
- **Invest in flexible solutions**