Deepfake ahead: Real fraud prevention in the AI era

Welcome to the era of synthetic reality

Today’s speaker

Julie Reynoso

Treasury Management Sales
U.S. Bank

What we’ll cover

- Fraud in the AI era
- Payments fraud
- Fraud controls
- Questions

Fraud in the AI era

Why should we care about fraud?

New Fraud "ecosystem"

- Large degree of specialization
- Supply Chain model

Increase in fraud events overall

- Social Engineering (bank impersonation campaigns)
- Mail theft (check fraud)
- Payment fraud (VEC)
- Ransomware

Short- and long-term impacts

- Potential for significant loss
- Reputation risk
- Data and systemic impact

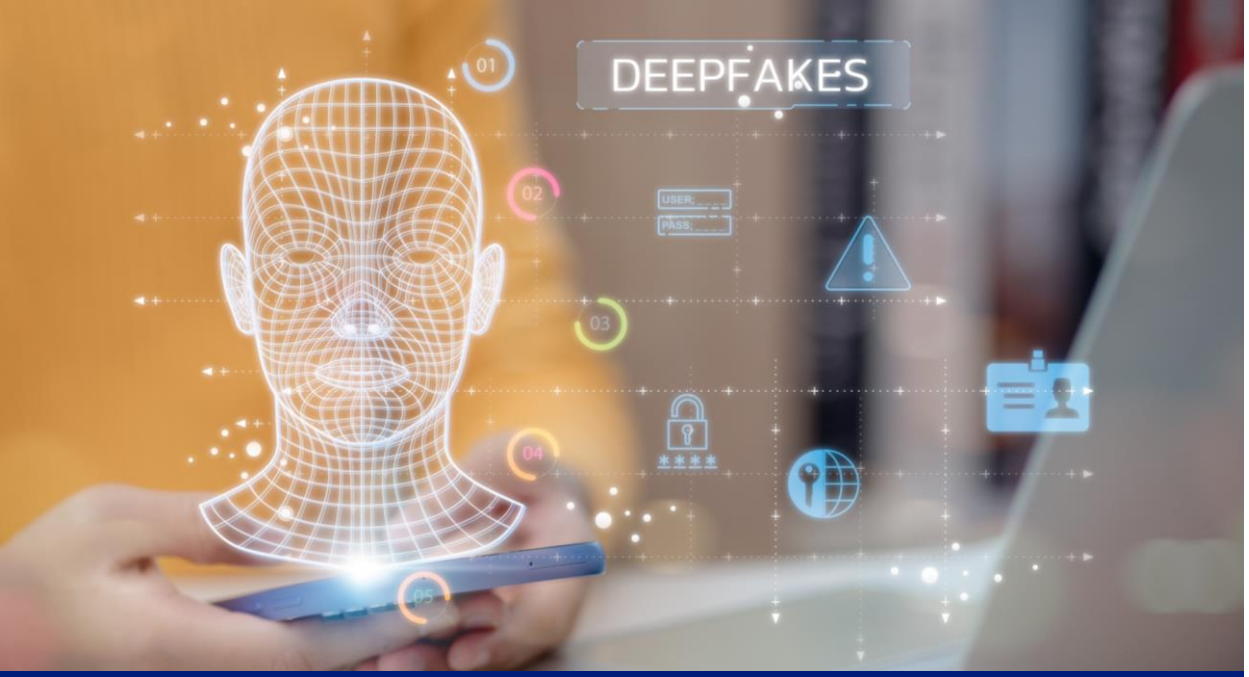
Fraud is a risk, not an event.

The wide spectrum of payments fraud

From low-tech
Mail Theft

To high-tech
Generative AI

Source : https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf
Source: https://www.cnbc.com/2024/02/14/gen-ai-financial-scams-are-getting-very-good-at-duping-work-email.html



Synthetic media

Synthetic media (aka Generative AI) threats permeate our technology via text, video, audio and images using techniques that damage an organization's brand; impersonate leaders and financial officers; and use fraudulent communications to gain access to an organization's networks, communications and sensitive information.

Source: CSI-DEEPFAKE-THREATS.PDF (defense.gov)

Capabilities

- Imagery
- Text
- Audio
- Video

Techniques

- Biometric bypass
- Zishing
- Deepfakes

Deepfake payments fraud in the headlines

World / Asia

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Source: https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Email compromise continues to grow and evolve

Email compromise is a type of cybercrime where attackers use various tactics, such as phishing and malware, to gain access to victims' email accounts. Once access is secured, attackers trick or threaten the target to make a fraudulent financial payment. Email compromise can include:

- Business Email Compromise (BEC)
- Email Account Compromise (EAC)
- Vendor Email Compromise (VEC)

21.5K

complaints in 2023.

$2.9B

in adjusted losses in 2023.

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

Email compromise has evolved into many variants

Business Email Compromise (BEC)

Impacts targeted organization and employee. Victim is typically employee following fraudulent payment instructions.

Email Account Compromise (EAC)

Impacts organizations and individuals (email owner and contacts) and can range from financial loss to data exposure

Vendor Email Compromise (VEC)

A scam where the fraudster impersonates a 'trusted' vendor/partner for financial gain. Impacts go beyond organization to affect clients and customers with potential financial loss and malware deployment

Vendor Email Compromise (VEC)

The difference between BEC and VEC

While traditional BEC attacks usually claim to be from a trusted individual within the organization, VEC goes one step further: it impersonates vendors (or other trusted third parties) to trick the target into paying fraudulent invoices, disclosing sensitive data or granting access to corporate networks and systems.

Research

Cyber actor conducts open-source research on awarded and ongoing projects and companies.

Domain registration

Cyber actor creates a spoofed domain like the legitimate company.

Business Email Compromise (BEC)

Cyber actor sends an email to a customer of the legitimate company requesting a change to the ACH payment or direct deposit information.

Information change

Customer believes the email is legitimate and changes banking information.

Transfer

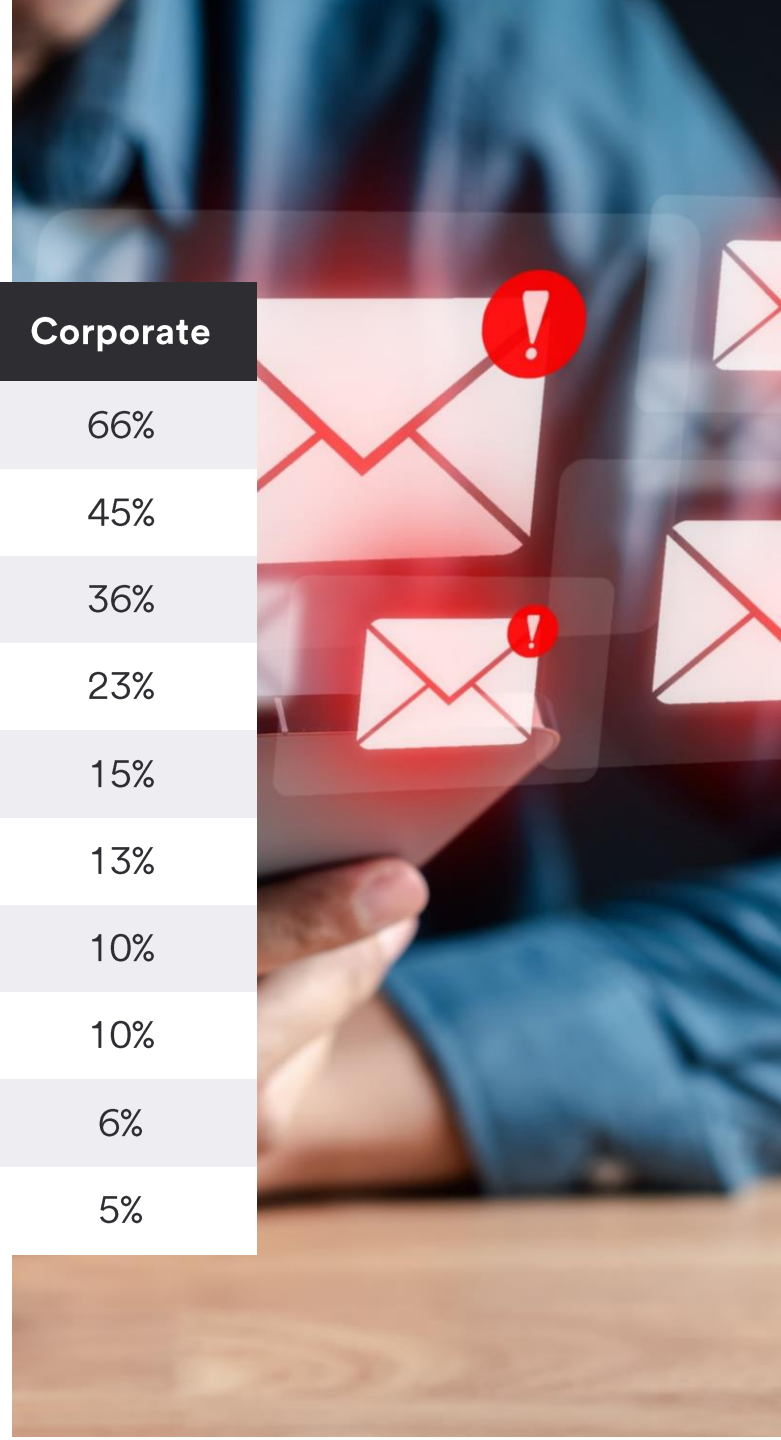
Customer transfers money to new account and the cyber actor receives the money.

Payments fraud

Sources of attempted/actual payments fraud

Percent of organizations

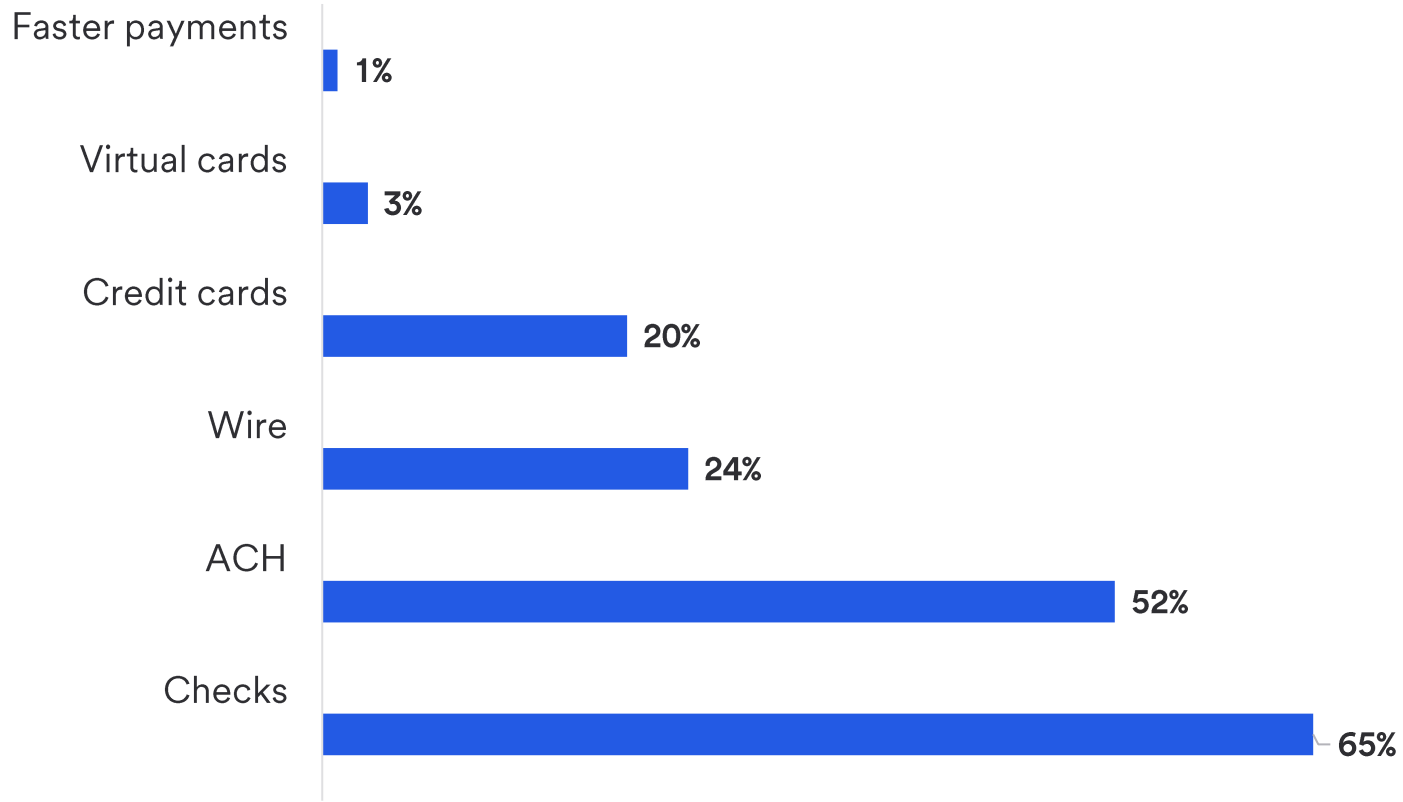
	All	Commercial	Corporate
Outside individual (e.g., check forged, stolen card, fraudster)	65%	63%	66%
Business Email Compromise (BEC Fraud)	38%	28%	45%
Vendor imposter	34%	31%	36%
U.S. Postal Service Office interference	21%	20%	23%
Invoice fraud	14%	14%	15%
Imposter to client posing as representative from our company	12%	9%	13%
Bad actor takes over an account (i.e., Account takeover)	10%	11%	10%
Third party or outsourcer (vendor, professional services provider)	10%	11%	10%
Organized crime ring	7%	10%	6%
Compromised mobile device (spoof/spam text message or call)	6%	8%	5%



Source: 2024 AFP® Payments Fraud and Control Survey Report
https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

Payment methods subject to fraud by type

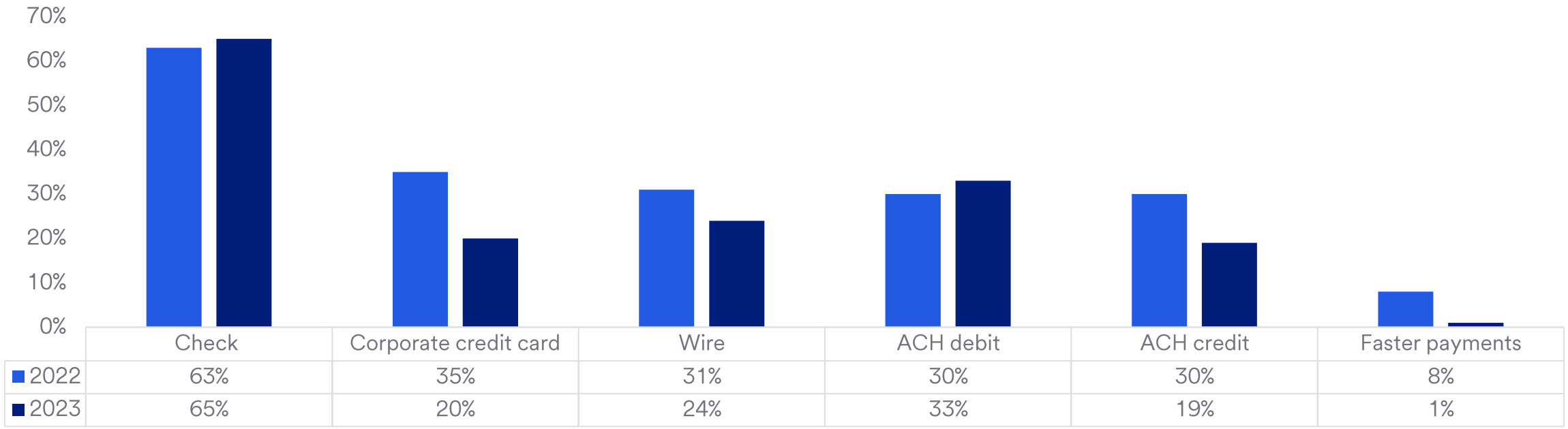
Percent of organizations



Source: 2024 AFP® Payments Fraud and Control Survey Report
https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

Checks and ACH continue to be the payment methods most impacted by fraud activity.

Trend comparison by payment type



	Check	Corporate credit card	Wire	ACH debit	ACH credit	Faster payments
2022	63%	35%	31%	30%	30%	8%
2023	65%	20%	24%	33%	19%	1%

Checks are most impacted by fraud due to low-cost and low-tech nature

Enhanced security technologies and MFA are more common

Good controls are in place with improved awareness of scams but remain vigilant

Tools like debit filters and blocks offer good control

Don't be fooled: in 2023 ACH overtook Wires as the most vulnerable to BEC

Be prepared to know what to look for as this category grows adoption in the United States

Source: 2024 AFP® Payments Fraud and Control Survey Report
https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

Fraud controls

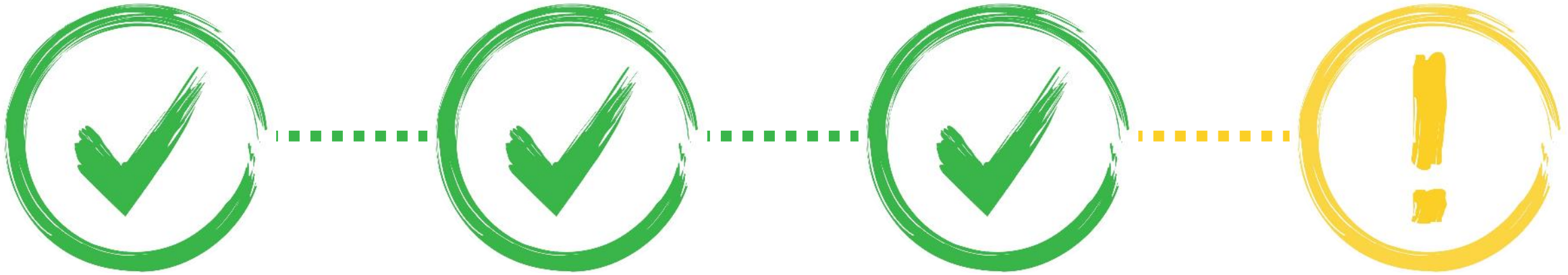
Mitigation

Validate

Validate

Validate

Only then send.



Synthetic media scam countermeasures

Review latest updates

Stay educated: review updates on the latest technology-based countermeasures.

Shared secret

Use shared secrets that should only be known internally to validate parties.

Never do

Supervisors should provide employees with guidance on actions they would never direct them to do.

Multi-person authorization

Having multiple eyes reviewing a transaction can substantially diminish likelihood of a fraud incident.

Multi-factor/multi-channel verification

Using a second form of authentication can prevent a substantial number of scams if the second factor is distinct from the primary.

Behavior-based detection and countermeasures

Pay attention to inconsistencies in the other person's story or actions.

Validate the destination of electronic payments

- As you move away from paper, leverage tools to validate recipient account status and/or ownership
- With Early Warning services, access a secure national shared database of checking and savings accounts to verify first before sending a payment
- Get real-time responses for any account-based transactions
- Avoid stress and cost of rejected transactions

Mitigate risk

Reduce potential financial loss

Minimize cost of exceptions

Ensure your banking partners have experience in dealing with payments fraud

Fraud prevention best practices

- Prioritize digital payment methods
- Incorporate a multi-layered process on significant transactions
- Train (and test) employees
- Automate high-risk tasks:
  - Outsource check printing
  - Seek partners to handle vendor onboarding and screening
- Incorporate a regular fraud checkup with your bank which should include:
  - Identify potential gaps in protection
  - Fraud solution demos
  - Handling of and timing to action exceptions
  - Setting defaults to not pay if deadlines are missed

Act immediately – have a plan for your fraud response

Contact your financial institution immediately, and request to open a fraud case

Contact your local FBI Office and file a complaint

Also file a complaint with the FBI's Internet Crime Complaint Center (IC3)

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

Additional questions