



NORWEGIAN MINISTRY
OF JUSTICE AND THE POLICE

Id-theft & the use of biometrics

*Magnar Aukrust
Deputy Director General*

The backdrop

- Increase in id-theft
- Increase in electronic communication & cross-border travel
- Increase in the use of different solutions for id verification and authentication, i.a. through use of biometrics

My presentation: Use of biometric identifiers as a means against id-theft?

- Biometrics are already in use for verification purposes, i.g. in travel documents.
- The current use of biometrics is strictly reserved to certain areas, partly because of privacy concerns.
- Can biometric be used on a broader scale without compromising privacy?
- As a privacy measure in itself?



GETTY IMAGES



GETTY IMAGES



Modern id-thefts I: Statistics etc.

- Financial & commercial fraud
- Posing as another when apprehended for a crime
- "Identity cloning" – facilitation of high level crimes

- -and the statistics? Volume of id-thefts?
Consequenses and losses for individuals, banks,
public security?

Modern id-thefts II: What do criminals need?

- Credit cards, id-cards, access cards, access devices.
- Names, addresses, date of birth, public registration numbers (social security numbers, medicare, tax, "fødselsnummer").
- Passwords, PIN codes, signatures etc.

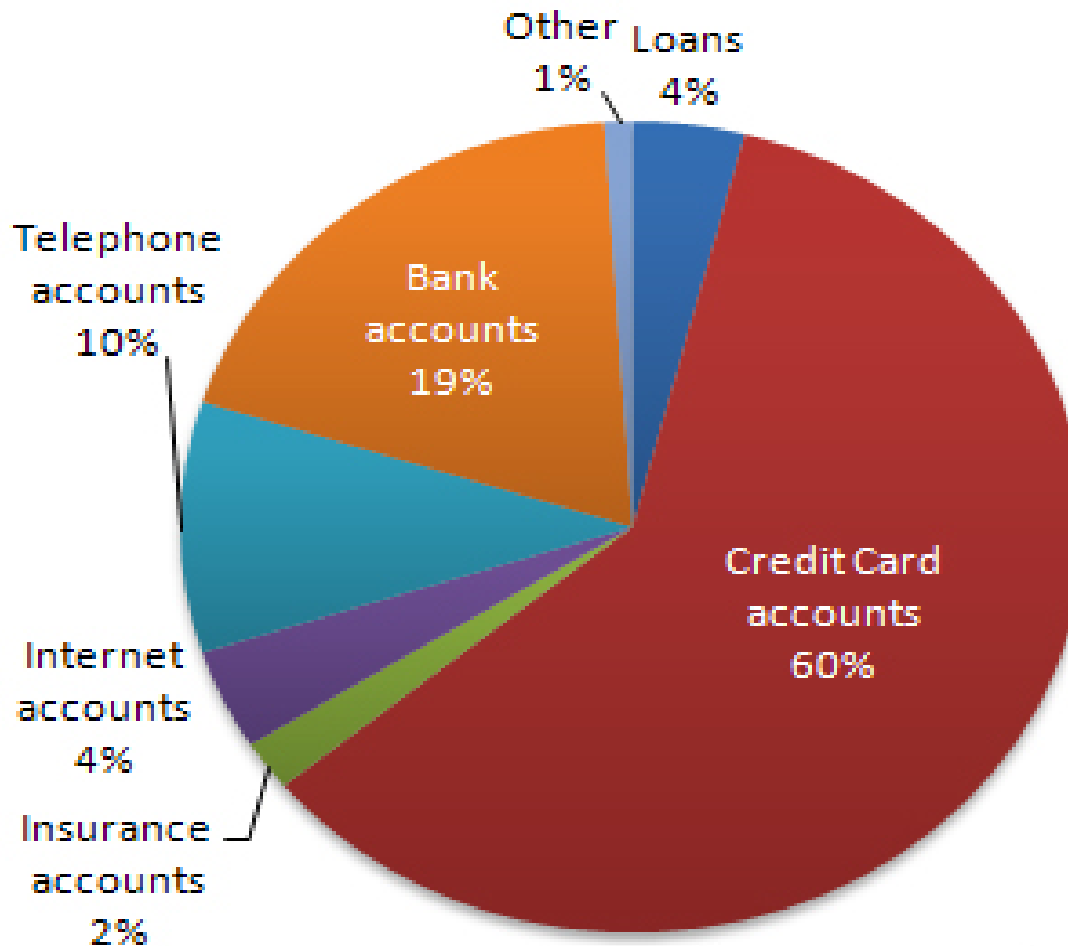
Modern id-thefts III: Methods – modus operandi?

- Hacking, skimming, phishing etc.
- Thefts – wallets, mail-boxes, PCs, cellphones etc.
- "Dumpster diving", dumped data retrieval.
- Illoyal employees, data breaches.
- False/fake identity manufacturing.

Modern id theft in a nutshell

- Criminals can use a lost or stolen creditcard – with your PIN code.
- You can have a problem proving it was not you
- Criminals can access your bankaccount(e.g. through hacking, malware etc. without your knowledge
- You can risk to be registered as a criminal because someone else has used your identity.

How was stolen information used?



In **20%** of cases, information was used to open **new** accounts in the victim's name.

Source: FraudWatch International - Types of Identity Theft

Id theft - conclusions

- Id theft is a big – and increasing - threat to individuals, financing and the society.
- Existing system for verification of ids and authentication on-line have loopholes which easily can be exploited by criminals.



Why did we get
there?

And how do we get out
of the quagmire?

The history behind the verification processes - I

- Early history of man: All transactions between people who knew each other and met in person
- Early Roman history: The use of witnesses
- From the Middle Ages to Modern Time: The use of signature (a biometric measure!).
- Conclusion: All obligations established through **personal presence** (and the signing of documents).

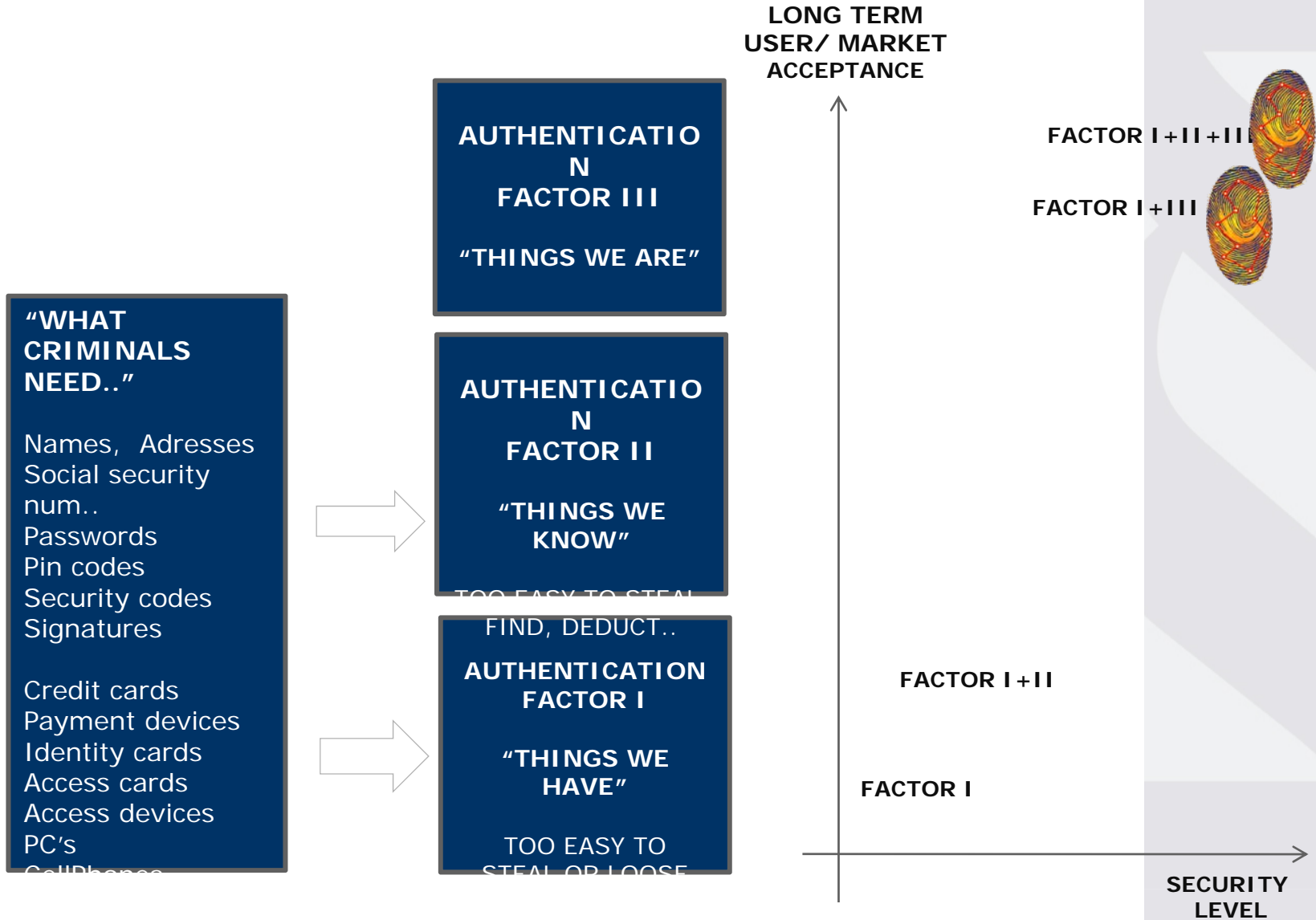
History of the verification process in the 20th century

- Developement of electronic communication & eCommerce. Without personal precence.
- New tech and laws to enable the use of digital signature (without physical signature)
- The use of cards and/or password/PIN cods in common use worldwide for signing.
- - and open for criminal attacs throught id-theft and other computer crimes!
- CAN ID-THEFTS BE AVOIDED BY THE USE OF BIOMETRICS AS A SUBSTITUTE FOR PERSONAL PRESENCE?

Re-introducing physical presense by use of biometrics?

- Combining something you *have* (Id-card) and/or
- with something you know, and add to this
- *something YOU ARE : One or more biometric identifiers.*

FIGHTING IDENTITY THEFT & IDENTITY FRAUD



Types of biometric – a lot of options

- Facial recognition
- Fingerprints (finger vein, hand geometry)
- Iris scan
- Retinal scan
- Voice recognition
- DNA
- *Signature*
- *Etc.*

Types of biometric applications

- Stored in cards (eID)
- Stored in databases
- Stored on cards, barcode or magnet strip
- Combining two or more biometrics
- Combining two or more media for storing – card/database – electronically/barcode etc

- Stored as an image
- Stored as a template.

Biometric as identifier - how and why to choose options

- Socio/ethical aspects . Threat against health etc.
- Feasibility
- Availability
- Cost effectiveness
- Etc.

The use of biometrics in travel documents etc.

- ePassports – more than 300 mill world wide.
- National ID cards
- Visas
- Frequent travellers program

- Permanent resident's permit, local border resident's permit
- Etc.

The rationale for the use of biometrics

- Security
- Cost effectiveness
- User friendly
- Convenient
- - and PRIVACY?

Biometrics and Privacy

- Biometrics which can be linked/traced to individuals are **personal data**
- Biometrics are not in it self sensitive data,
- but awarenes against disclosure, intgrity and authencity important.
- Biometrics could be misuse, functional creep (e.g. fingerprint stored for verification purposes but used for criminal investigation.

- **Biometrics can also support privacy.**

- **The balance of intrest!**

Can biometrics also support privacy?

- Using a stolen e-Ids will be more difficult, and easier to detect.
- Electronic tracks left by the use of Id cards with biometrics impossible.
- ID fraud by the use of biometric identifiers impossible
- Etc.

- But still a lot of loopholes

And how can we take care of privacy when using biometrics?

- Personal data security
- Physical and organisational protection
- Encryption, BAC, EAC

- Generating an access code (template) from a biometric identifier which can not be restored as a biometric (e.g.. a fingerprint)

- Conclusion: Use of privacy enhancing technologies (PET)

Conclusions on the use of biometrics

- The use of biometrics can be an efficient tool against it-theft and id-fraud.
- Biometrics can be used in privacy friendly manner.

Using existing id-document for "new" verification and authentication purposes:

- Passports? National Id-cards?
- What are the possibilities and limits?
- Can we store biometrics outside the chip restricted to official use?
- Can the private sector, banks etc. get access to a "proved" id established through a secure id process, e.g. In connection with the issuing of a card with a biometric based pincode?
- **THE CHALLENGE:** How to exploit existing systems without compromising privacy and information security?

The future

- Building trust by the use biometrics as an authentication method,
- Avoiding privacy and information security threats by appropriate technologies,
- Enhance cost effectiveness and convenience by re-useing existing biometric and identity management systems,

TO MEET THE THREAT AGAINST PRIVACY FROM
MODERN FORMS OF ID-THEFT!

And how to get there?

- Initiatives from different stakeholders.
- Promoting the development of privacy enhancing technologies.
- Prepare – nationally and internationally – appropriate legal framework.

- Governmental id cards?

CONCLUSION

- We have the tool to prevent id theft
- JUST USE IT!

THANK YOU FOR
YOUR ATTENTION

?

magnar.aukrust@jd.dep.no





HAVE A NICE DAY !