RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: AFD-T08

Balancing UX and Secure Banking in a Fast Transforming Industry

Boudewijn van der Valk

Chapter Lead Fraud Prevention
ING

The digitization of the financial industry results in a big improvement of the user experience

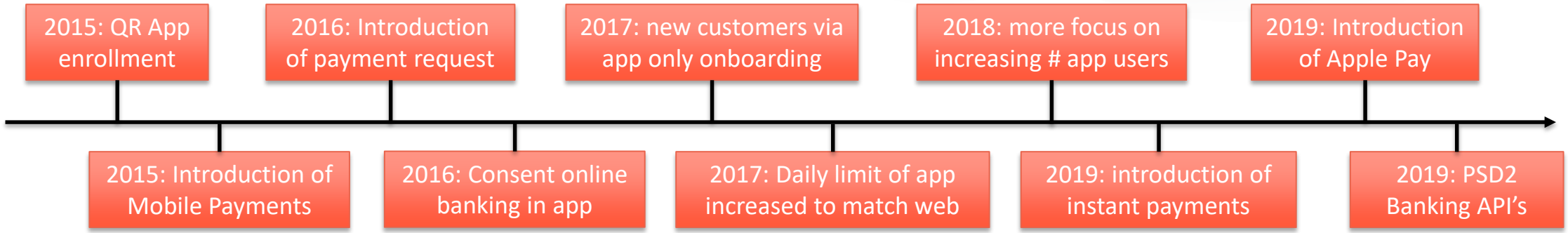
Customers expect a similar banking experience compared to their Google, Facebook, Amazon experience

But do customers still know how to remain safe?

Topics for today…

- What has changed -and why-, in our authentication & security landscape due to digitization and regulation?
- Which Modus Operandi development do we see because of digitization and how do we counter them?
- How do we ensure that our traditional and new-to-digital group of customers are protected against cybercrime?

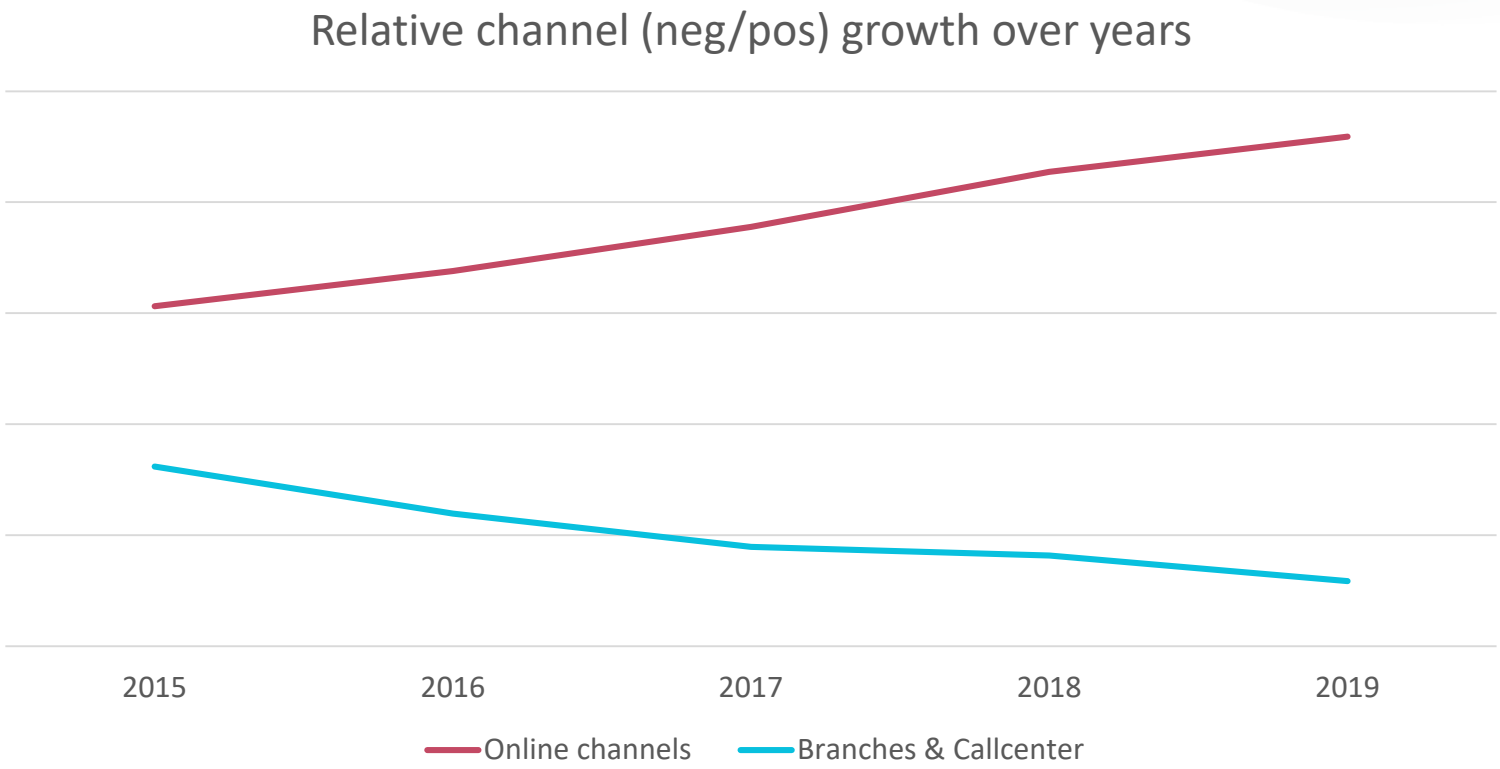
Prior years we saw a focus on digitization and more efficient processes



Prior years we saw a focus on digitization and more efficient processes

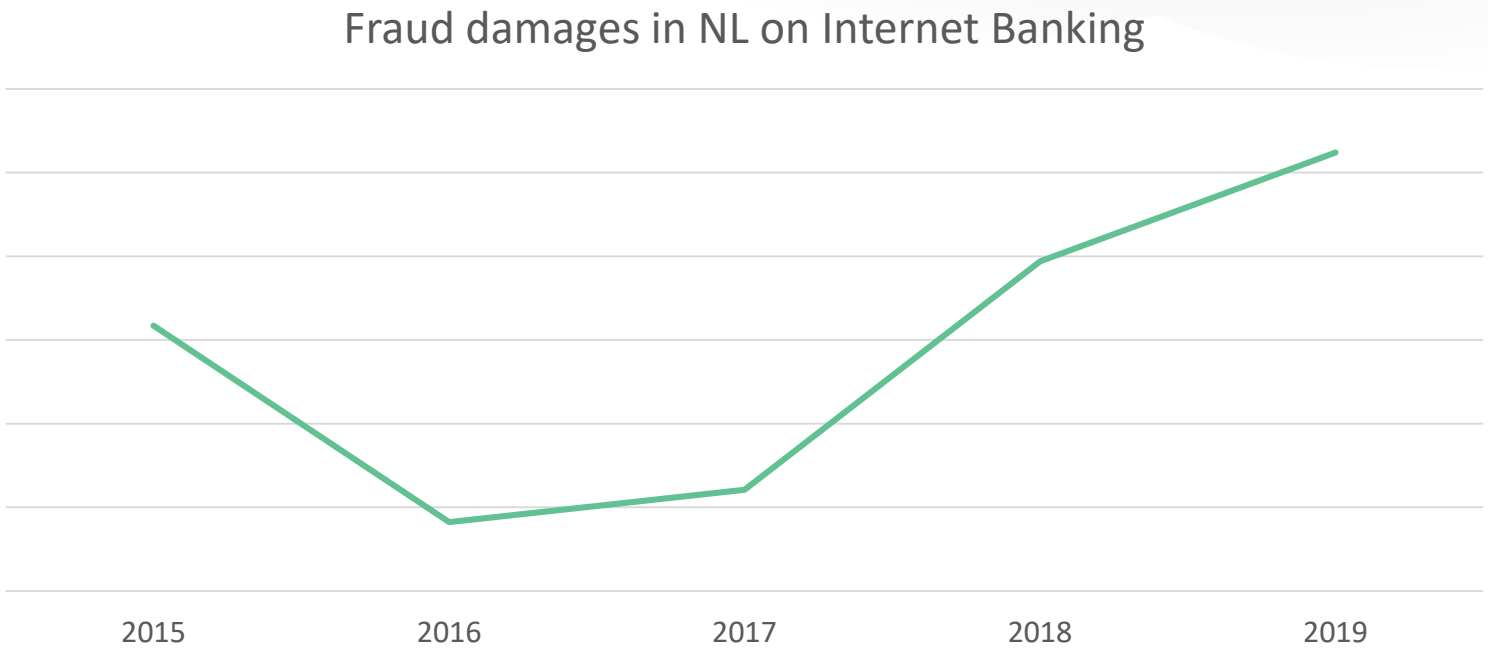
- 2015: QR App enrollment
- 2015: Introduction of Mobile Payments
- 2016: Introduction of payment request
- 2016: Consent online banking in app
- 2017: new customers via app only onboarding
- 2017: Daily limit of app increased to match web
- 2018: more focus on increasing # app users
- 2019: introduction of instant payments
- 2019: Introduction of Apple Pay
- 2019: PSD2 Banking API's

This led to an increased number of digital interactions



Source: Internal ING data

New Modus Operandi have resulted in increases in fraud



Source: Combined fraud report of Dutch banks, as published by Dutch Payment Association
https://factsheet.betaalvereniging.nl/en/

What we've seen so far

- The number of digital interactions have increased while the number of 'traditional' interactions have decreased
- We've added lots of functionality to the mobile banking app that has greatly improved the user experience in most daily banking processes
- However, this has resulted in fraudsters switching their focus to:
  gaining access to a user's mobile banking environment

RSAConference2020

How has fraud evolved in the era of digitization?

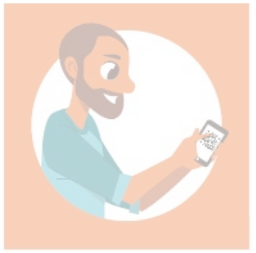
Focus on new Modus Operandi

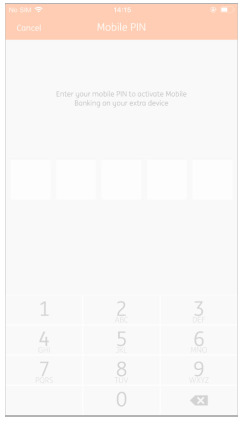
QR code enrollment flow to add 2nd app

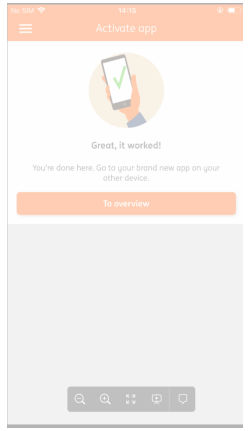
"Hey, can you pay this train ticket for me in cash? I can pay you back immediately via my phone"

Fraudster configures new device, sets new pin etc and can transfer money

"Sure, no problem. How would you pay me back?"

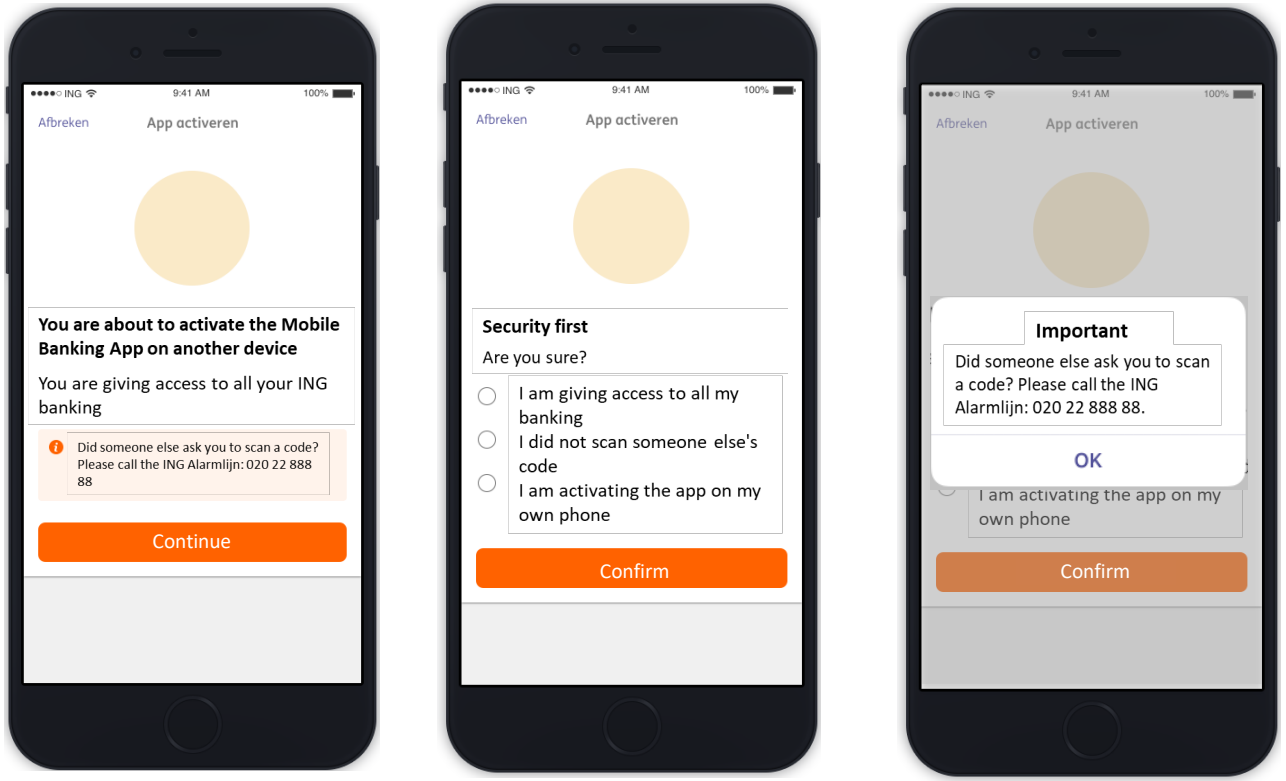






Confirmation SMS is sent that new device has been activated

Extra confirmation had to be added to raise awareness



- Extra confirmation on customers' device before enrollment could be completed
- Victim profile characteristics:
  - Happens in all age groups
  - Time of usage of app doesn't seem to be a factor

Payment request to ‘secure account’

Payment request to ‘secure account’


Uw vermogen veiligstellen

Geachte [redacted]

U heeft ons vermeld dat u teruggebeld wilt worden over het geld dat binnenkort wordt afgetrokken van de rekening [redacted] Deze mail ontvangt u om u te wijzen naar de pagina waar u uw geld veilig kunt stellen. Wij raden u aan dit zo spoedig mogelijk te doen.

Wilt u dat nu gelijk doen?

Klik dan hier om uw geld veilig te stellen. Wij verzoeken u dit zo spoedig mogelijk te doen.

Met vriendelijke groet,

Micheal Fluitsma

ING Security

- Victim profile characteristics:
  - Almost all victims were > 70 years old

WhatsApp / Messenger contact to transfer money

Hey Max, this is Daniel. My phone just broke down, this is my new number. Please remove the old one!

Yes, will do! What's wrong? Couldn't transfer your number?

Too much hassle, decided to go for a new numer

Everything OK?

Did you just try to call me with a hidden number?

No, wasn't me… but I'm good, thank you!

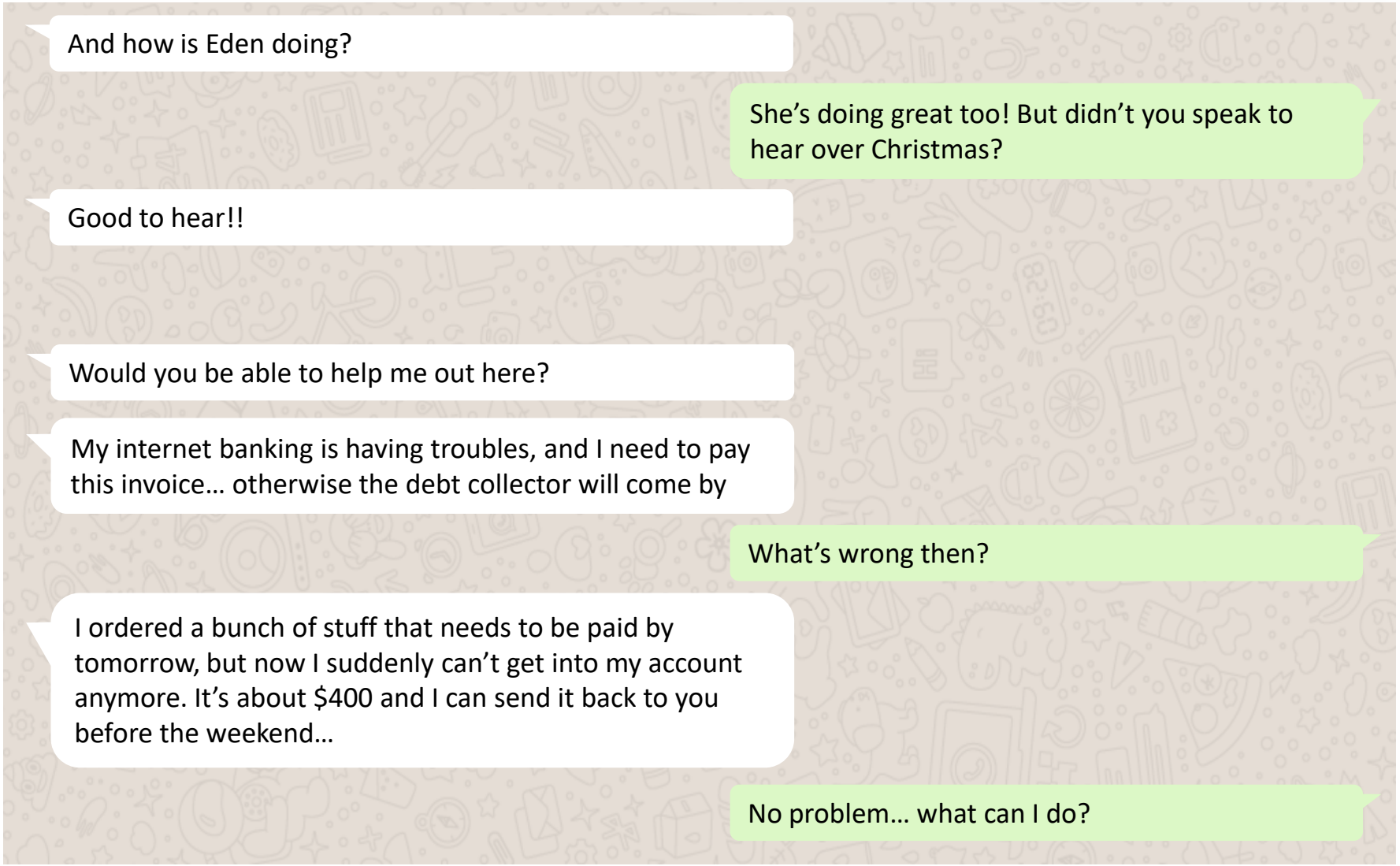
About to start with my thesis.. How are you?

Good to hear! I'm good too!

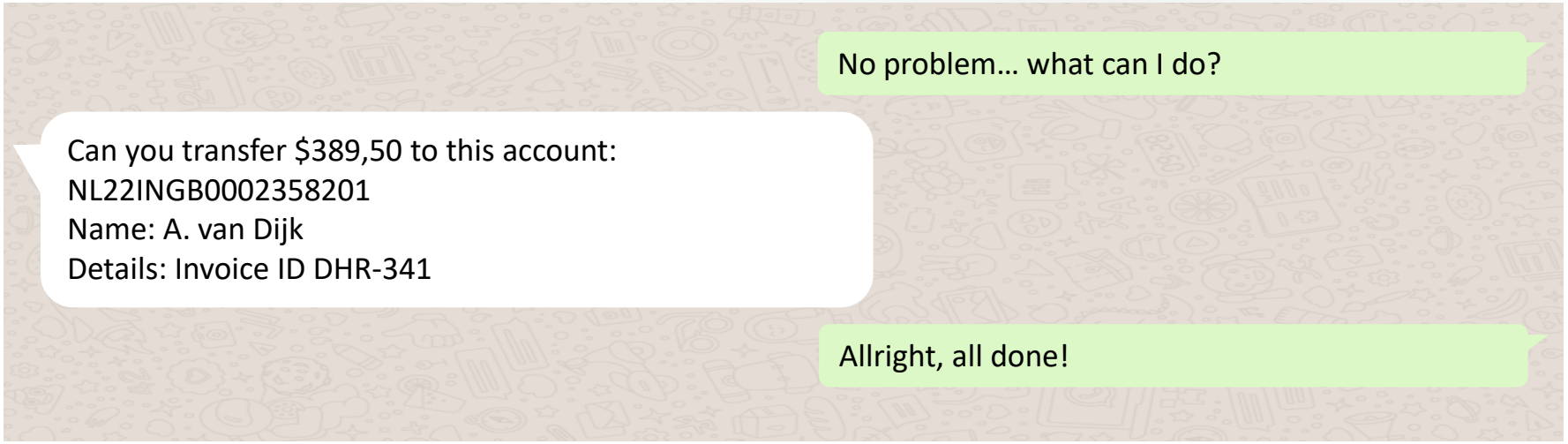
And how is Eden doing?

She's doing great too! But didn't you speak to hear over Christmas?

WhatsApp / Messenger contact to transfer money



WhatsApp / Messenger contact to transfer money



- Contact from (alleged) well known friend or relative
- Confidence by using information found on social media

- Victim profile characteristics:
  - 30% of victims are aged 50-65 y/o. Hypothesis: parents thinking they're helping their children
  - Customers that have recently started to use our app do not appear to be more vulnerable

RSAConference2020

How has fraud evolved in the era of digitization?

Cash out enablers

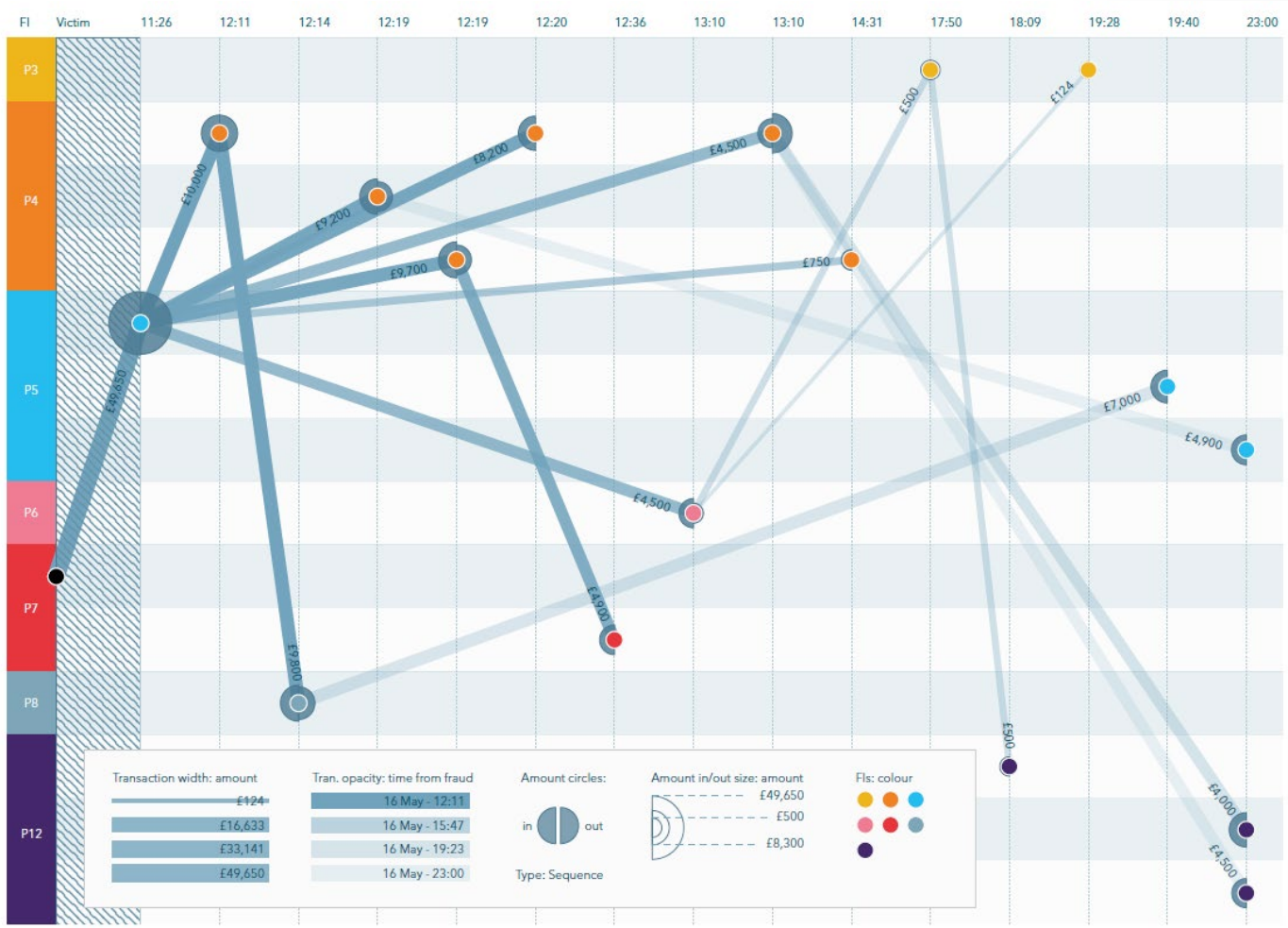
Mobile apps offer more functionality

- Mobile wallets to add POS payment functionality
- App also used for consent in web
- Payment requests are very well known in The Netherlands, allows for fake payment requests
- Debit / Credit card settings can be changed
- Address can be changed, risk of fraudulent new product agreements
- Use SSO functionality into web environment to gain access to all online functionality

Instant Payments could make cashout easier

- Previously, fraudsters preferred to have mule accounts at the same bank as their victims due to the speed of money transfers
- With the introduction of instant payments this is no longer required
- We expect to see complex mule networks with multiple levels, where:
  - mules at the front of the chain are cheap and easy to swap, and
  - mules deeper in the network are most valuable and used for cash-out
- To improve detection, Dutch banks are working on adding the ‘Fraud Indication Marker’ to all Instant Payments

Example: hiding money from investigations using mule network



Source: Rise of the Mule, Mastercard / Vocalink
https://www.mastercard.us/content/dam/mccom/en-us/documents/vocalink-anti-money-laundering-case-study.pdf

RSA Conference 2020

How to protect our customers?

How can we protect our customers?

- When performing consent, provide clear verification information about the transaction
- Offer a primary authentication avenue but enable alternatives for customer groups that can't or really don't want to use it
- Consistent communications: If we say 'we will never ask you to login through an e-mail or SMS', make sure we don't
- Central and up to date page to provide customers information about secure banking

How can we protect our customers?

- Work together with other banks for broader campaigns
  - All safe banking campaigns in Dutch media originate from the Dutch Payment Association, with input from participating banks
- Work together with community organizations and interest groups to raise awareness for specific groups of customers
- Warn specific target groups for specific MO’s

How can we protect our customers?

- To decrease risk of fraudulent app enrollment we will require a non-phishable means during app (re)enrollment flow
  - Government ID read-out using NFC and/or camera
  - Biometrics
- Keep authentication options clear and easy, so customers know what to expect
- Authentication avenues should be usable over multiple channels

RSAConference2020

Conclusions

Back to our question…

But do customers still know how to remain safe?

Apply this information to your organization

- Short term actions:
  - Re-assess your risk appetite and validate that added functionalities and growth of online channels are still represented correctly
  - Evaluate the increased vulnerabilities you experience, when phishing or social engineering schemes turn more personal and face-2-face
  - Increase effort to make customers more aware of what they're giving consent to and how to confirm that they're on the correct site
- Long term actions:
  - Consider non-phishable authentication means and where they should play a role in your online eco-system