

# Shut Up and Take My Money!

*The Red Pill of N26 Security*

---



Vincent Hauptert

December 27, 2016

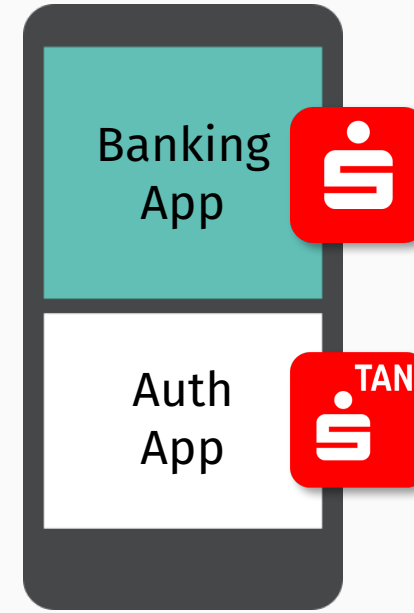
Security Research Group

Department of Computer Science

Friedrich-Alexander University Erlangen-Nürnberg



**Two-Device Authentication**



**Two-App Authentication**

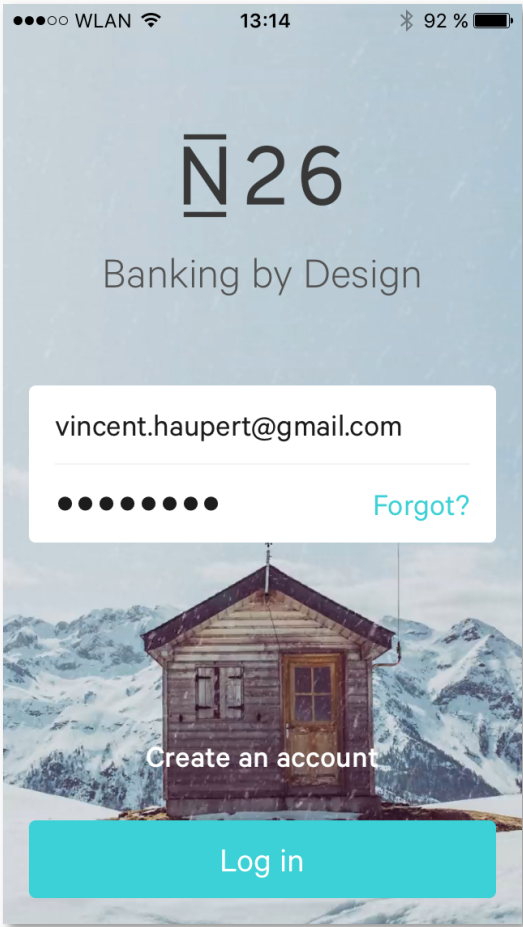


**One-App Authentication**

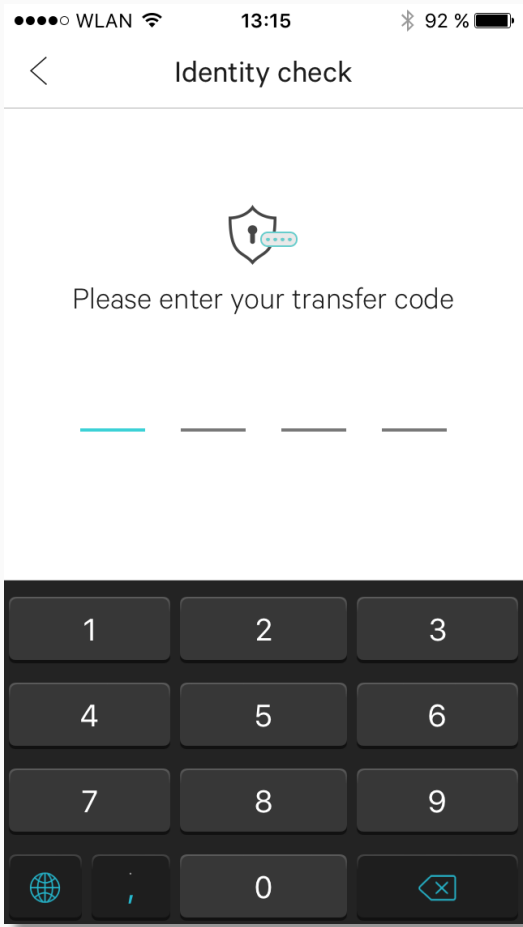
- Berlin-based “Mobile First” FinTech
  - German bank account
  - Smartphone as financial hub
  - Do *everything* with the N26 app
- Founded in 2013
- Over 200.000 customers
- Has its own European banking license
  - N26 Bank
  - Available in 17 countries
- Open a bank account in just 8 minutes



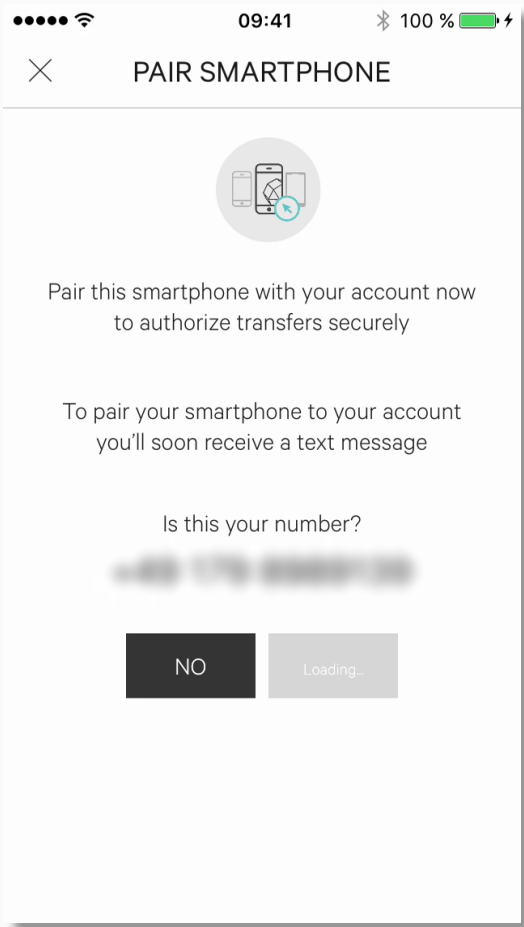
# N26: Transaction Security



Email & password



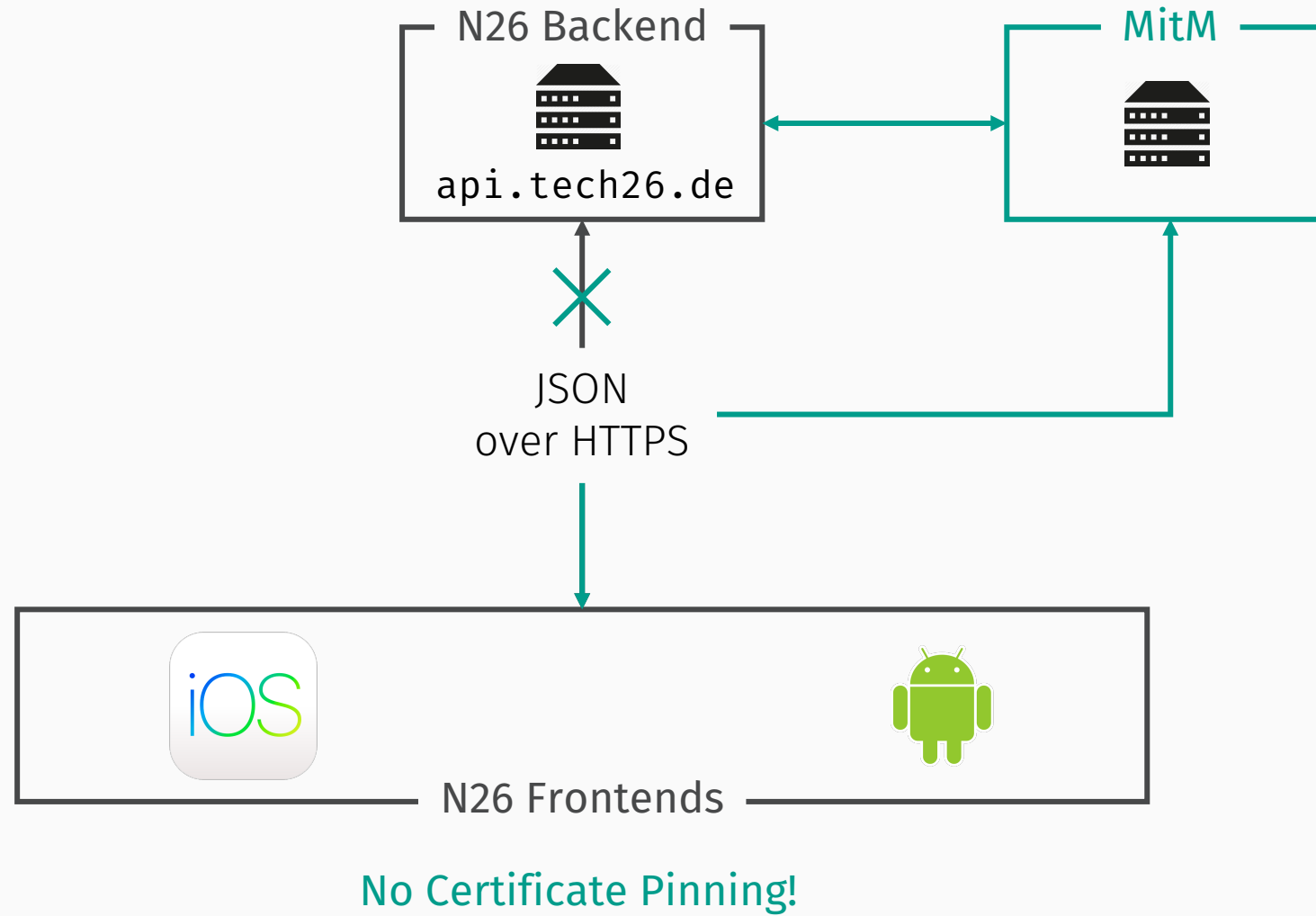
Transfer code



Paired phone

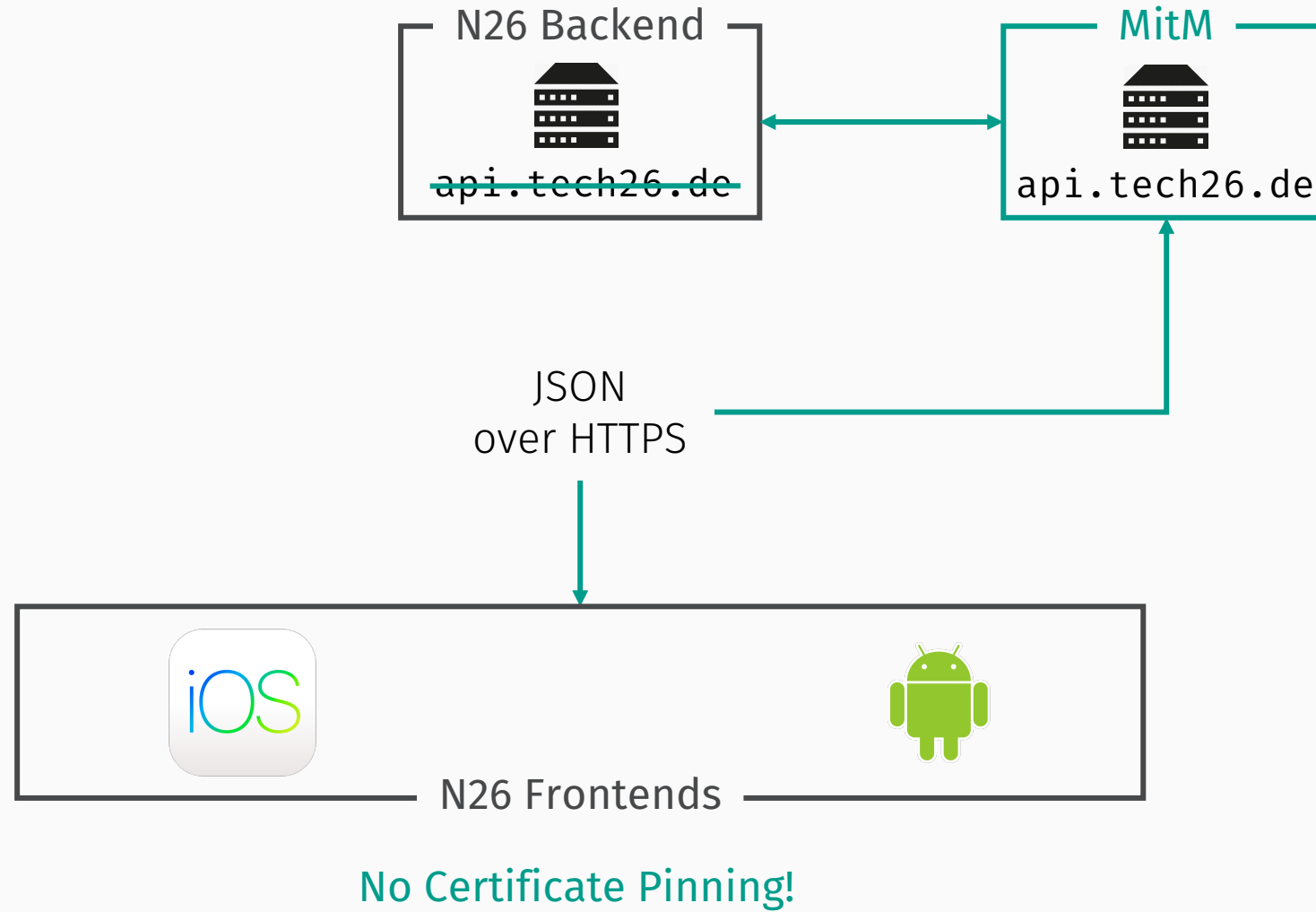


# N26 Architecture

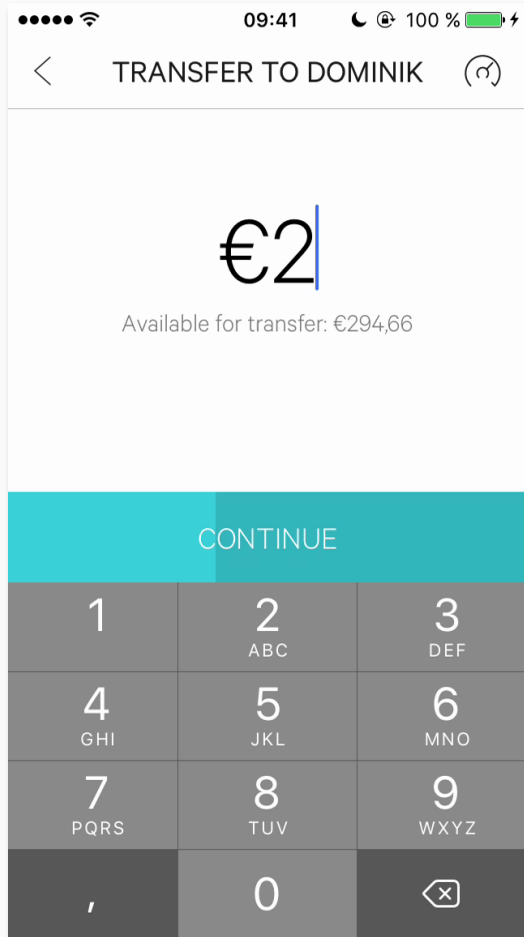


# Real-time Transaction Manipulation

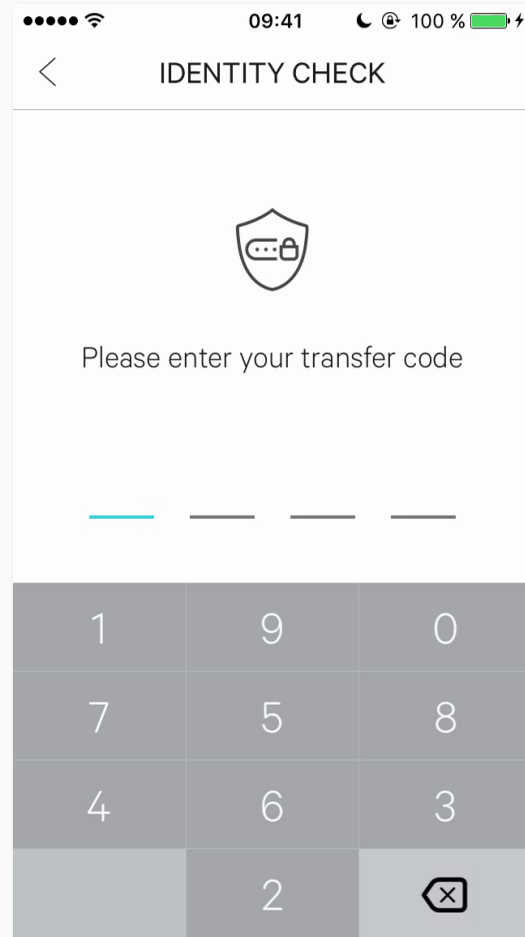
# Real-time Transaction Manipulation



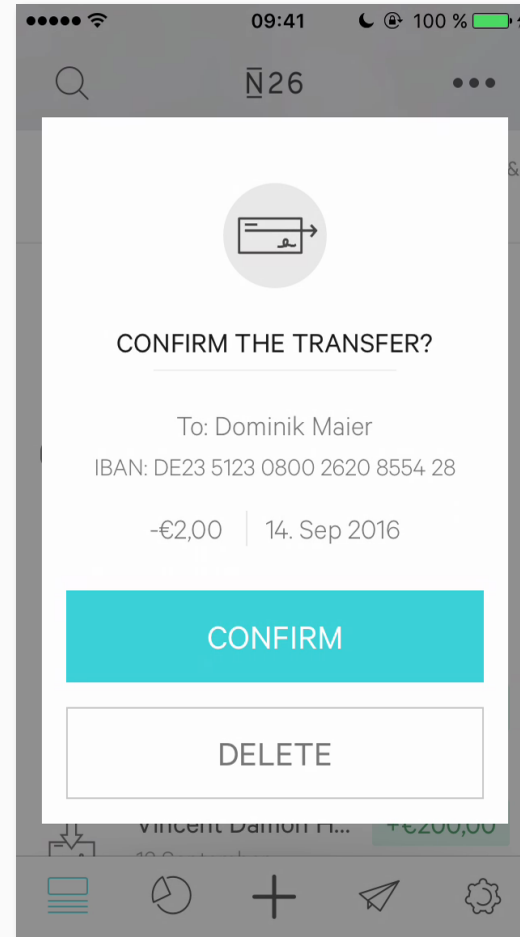
# Real-time Transaction Manipulation



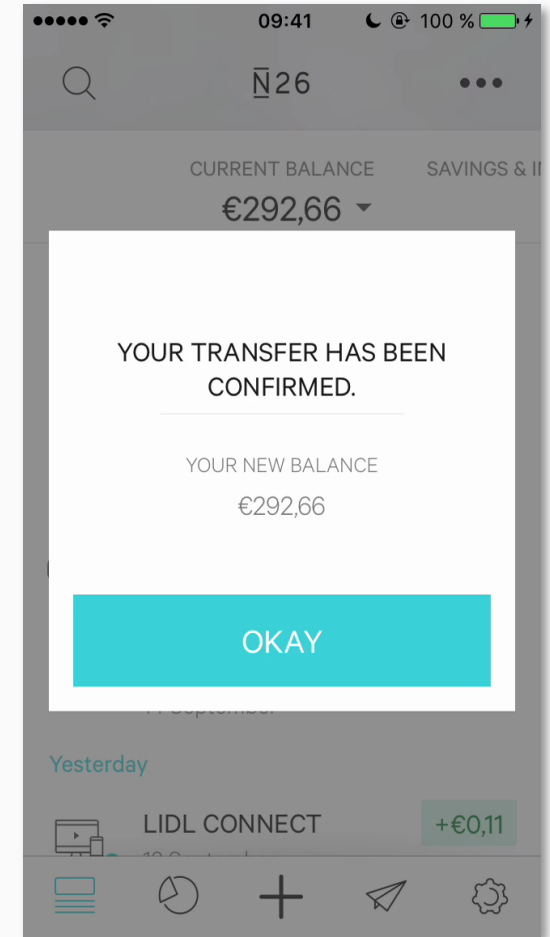
Transfer €2,00 to  
Dominik



Enter transfer code

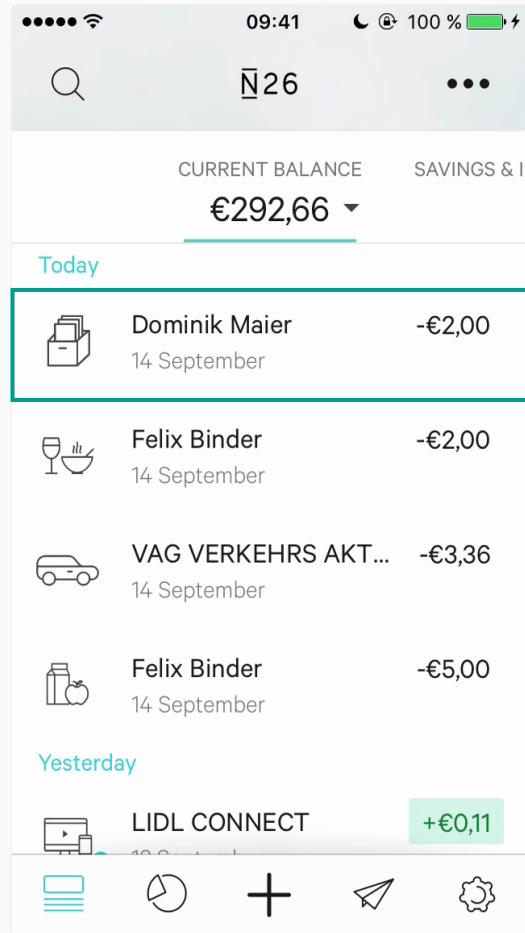


Confirm transfer








Confirmed:  
 $€294,66 - €2,00 = €292,66$

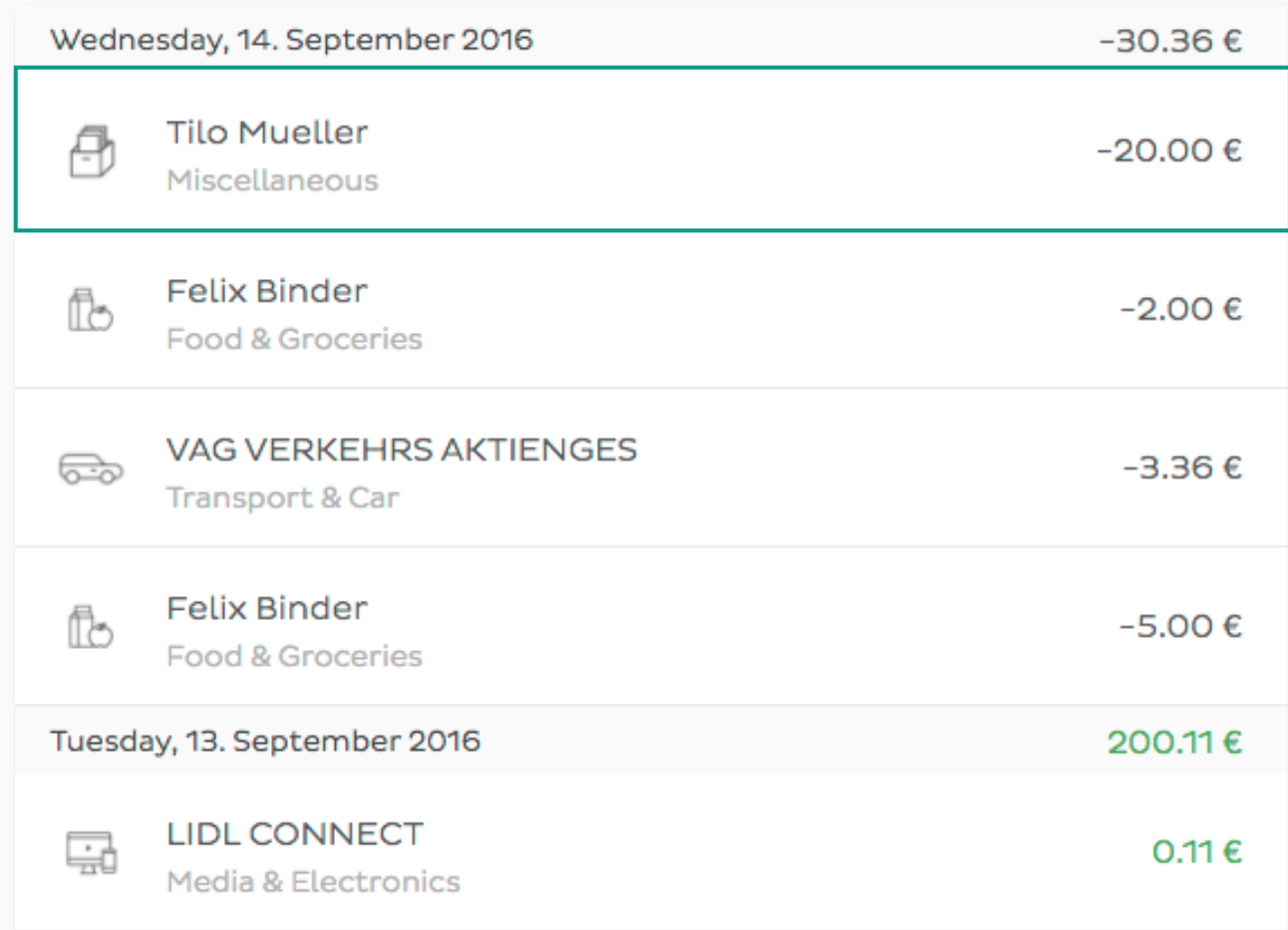
# Real-time Transaction Manipulation








A screenshot of a mobile banking app showing a transaction overview. The current balance is €292,66. The transactions are listed for 'Today' and 'Yesterday'. The first transaction in 'Today' is highlighted with a green border.

| CURRENT BALANCE  |                                     | SAVINGS & I |
|--|-------------------------------------|-------------|
| €292,66  |                                     |             |
| Today  |                                     |             |
|   | Dominik Maier<br>14 September       | -€2,00      |
|   | Felix Binder<br>14 September        | -€2,00      |
|   | VAG VERKEHRS AKT...<br>14 September | -€3,36      |
|   | Felix Binder<br>14 September        | -€5,00      |
| Yesterday  |                                     |             |
|  | LIDL CONNECT<br>13 September        | +€0,11      |

Transaction overview  
seems correct



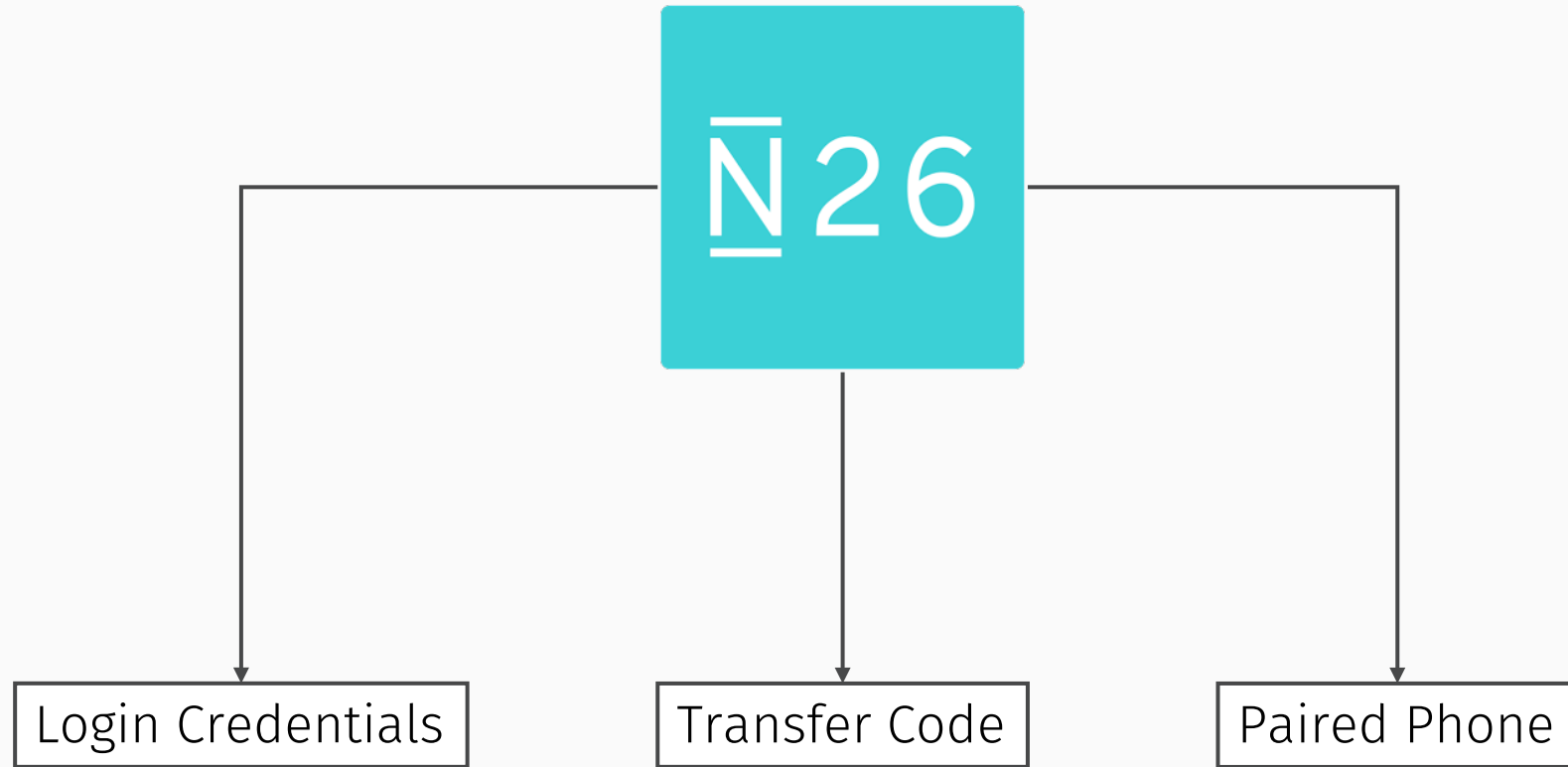
A screenshot of a detailed transaction list for Wednesday, 14. September 2016. The transactions are listed with their respective amounts. The first transaction is highlighted with a green border.

| Wednesday, 14. September 2016   |   | -30.36 € |
|---|---|----------|
|    | Tilo Mueller<br>Miscellaneous             | -20.00 € |
|    | Felix Binder<br>Food & Groceries          | -2.00 €  |
|    | VAG VERKEHRS AKTIENGES<br>Transport & Car | -3.36 €  |
|    | Felix Binder<br>Food & Groceries          | -5.00 €  |
| Tuesday, 13. September 2016   |   | 200.11 € |
|  | LIDL CONNECT<br>Media & Electronics       | 0.11 €   |

After the attack:  
€20,00 to Tilo instead of €2,00 to Dominik

# Account Hijacking

# Account Hijacking

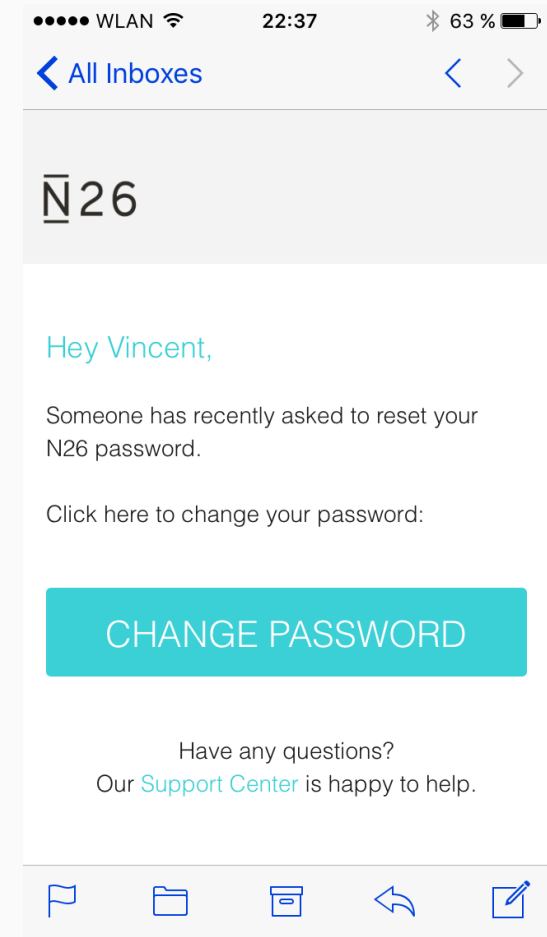


# Account Hijacking

— Login Credentials —



- “I forgot”: Recovery from Loss
  - Reset password only through email access
  - Breaks N26' password policy
- Spear phishing
  - Similar domain
  - Expose N26 customers
  - A valid reason to contact them

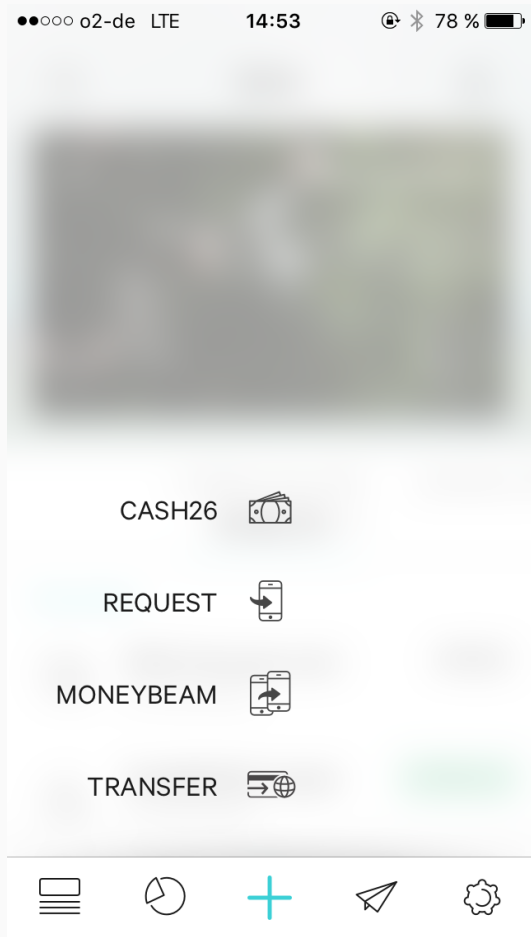


# Spear Phishing: Similar Domain

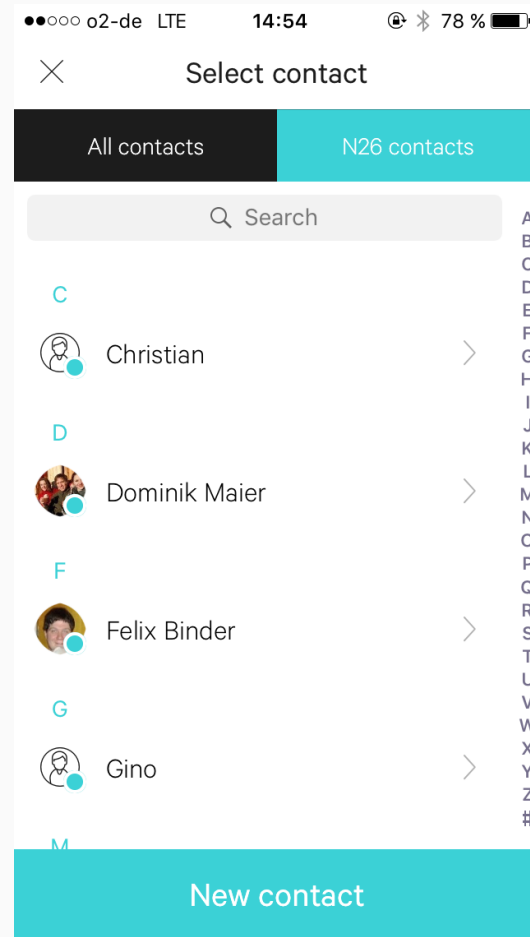
number26.tech

```
# whois number26.tech
Domain Name: NUMBER26.TECH
Name: Vincent Haupt
Registrant Organization: University of Erlangen-Nuremberg
Registrant Street: Martensstrasse 3
Registrant City: Erlangen
Registrant Postal Code: 91058
Registrant Country: DE
Registrant Email: vincent.haupt+n26@cs.fau.de
```

# Spear Phishing: Expose N26 Customers



MoneyBeam:  
P2P Transactions



Uploads your  
contacts

- Use this to identify customers of a given dataset



- Over 68M accounts leaked
- We evaluated *all* of them
  - No limits, no notice
- *Result:* Over 33.000 are N26 customers
- Also offers a valid reason to contact customers

# Spear Phishing

● N26

Please change your password

To: Vincent Hauptert

23 December 2016 at 22:36

N

Click here to change your N26 password:

CHANGE PASSWORD



[https://number26.tech/?  
email=vincent.hauptert@gmail.com](https://number26.tech/?email=vincent.hauptert@gmail.com)

Have any questions?

Our [Support Center](#) is happy to help.

Our [Support Center](#) is happy to help.

# Siri Transactions

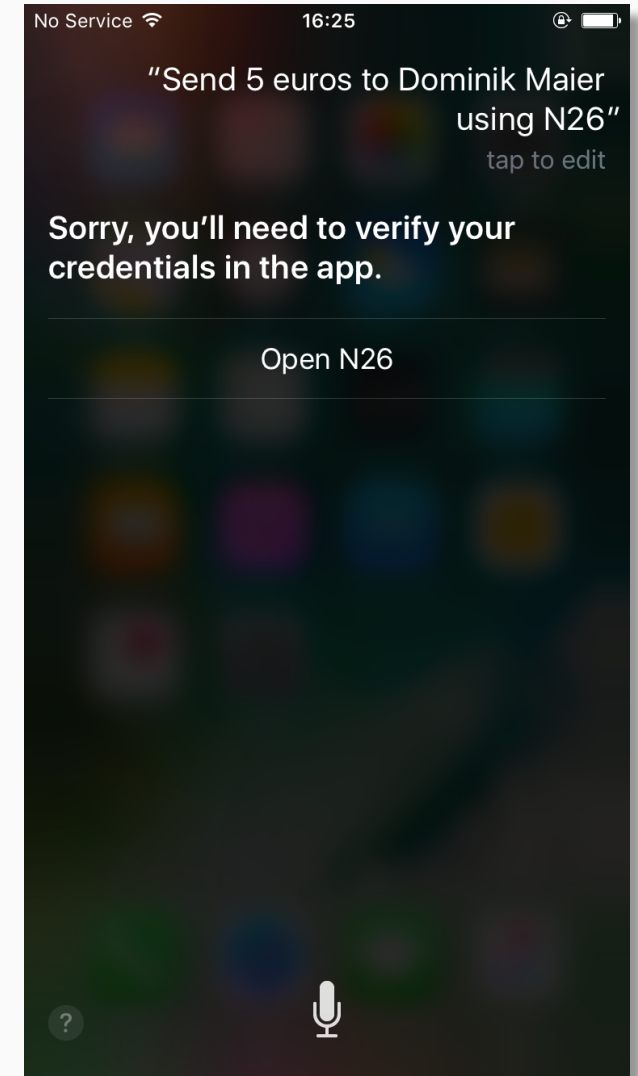
# Siri Transactions

- Since iOS 10, N26 supports Siri transactions
- Only the paired phone can send Siri transactions

`https://api.tech26.de/api/transactions/unverified`

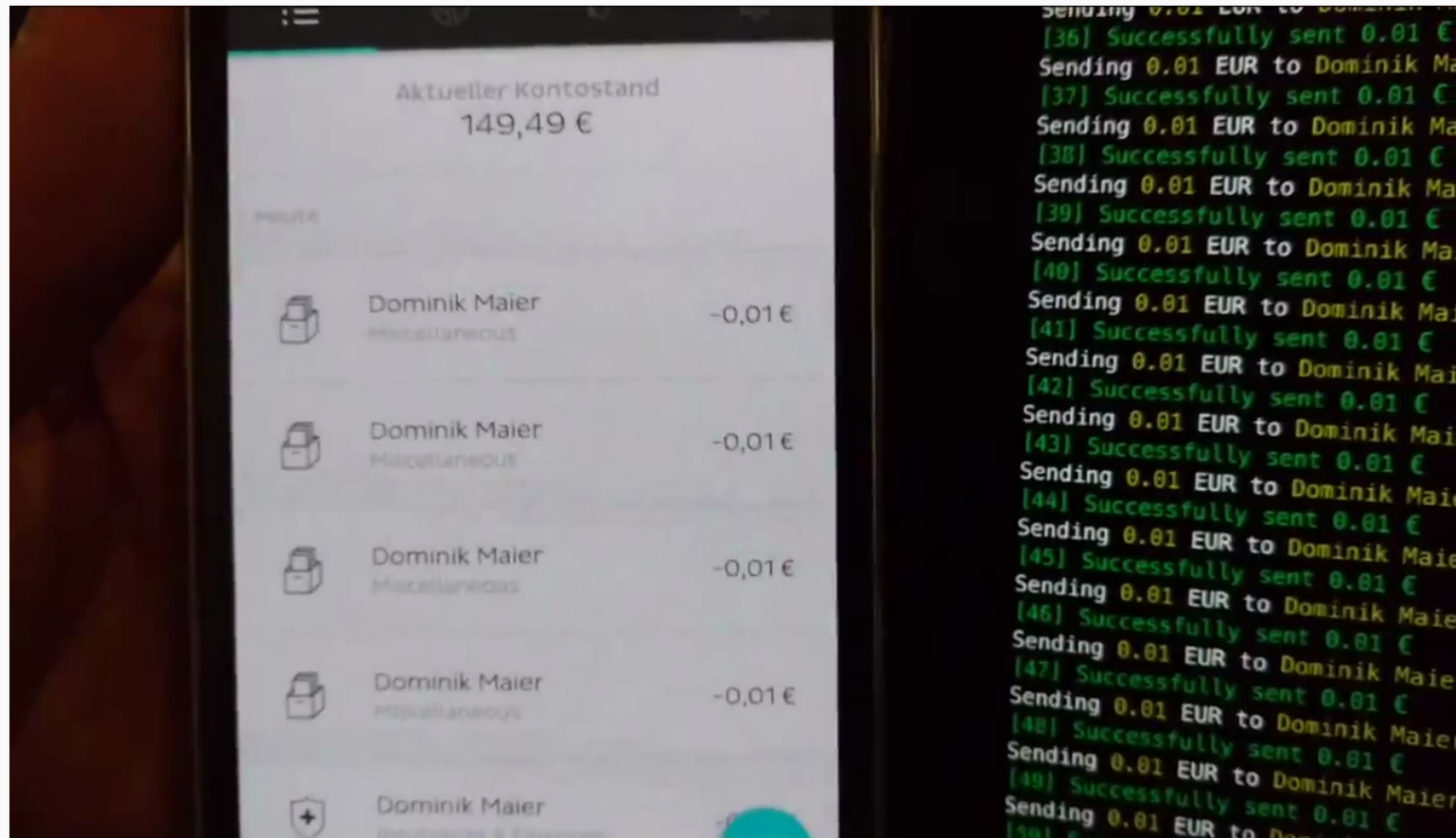
```
{  
  "amount": 5.0,  
  "partnerName": "Dominik Maier",  
  "partnerPhone": "+49*****74",  
  "type": "FT"  
}
```

Siri transactions don't require the paired device!



# Siri Transactions: Intelligent Algorithms

- N26 claims that it “*immediately detects irregularities*”
- Issued over 2000 transactions worth €0,01 within 30 minutes



# Siri Transactions: Intelligent Algorithms

- Transactions went through without a problem
- Over 3 weeks later, N26 required Dominik to explain the “unusual amount” of transactions
- N26 even wanted to cancel his account

Dominik, however, didn't send but receive the money!

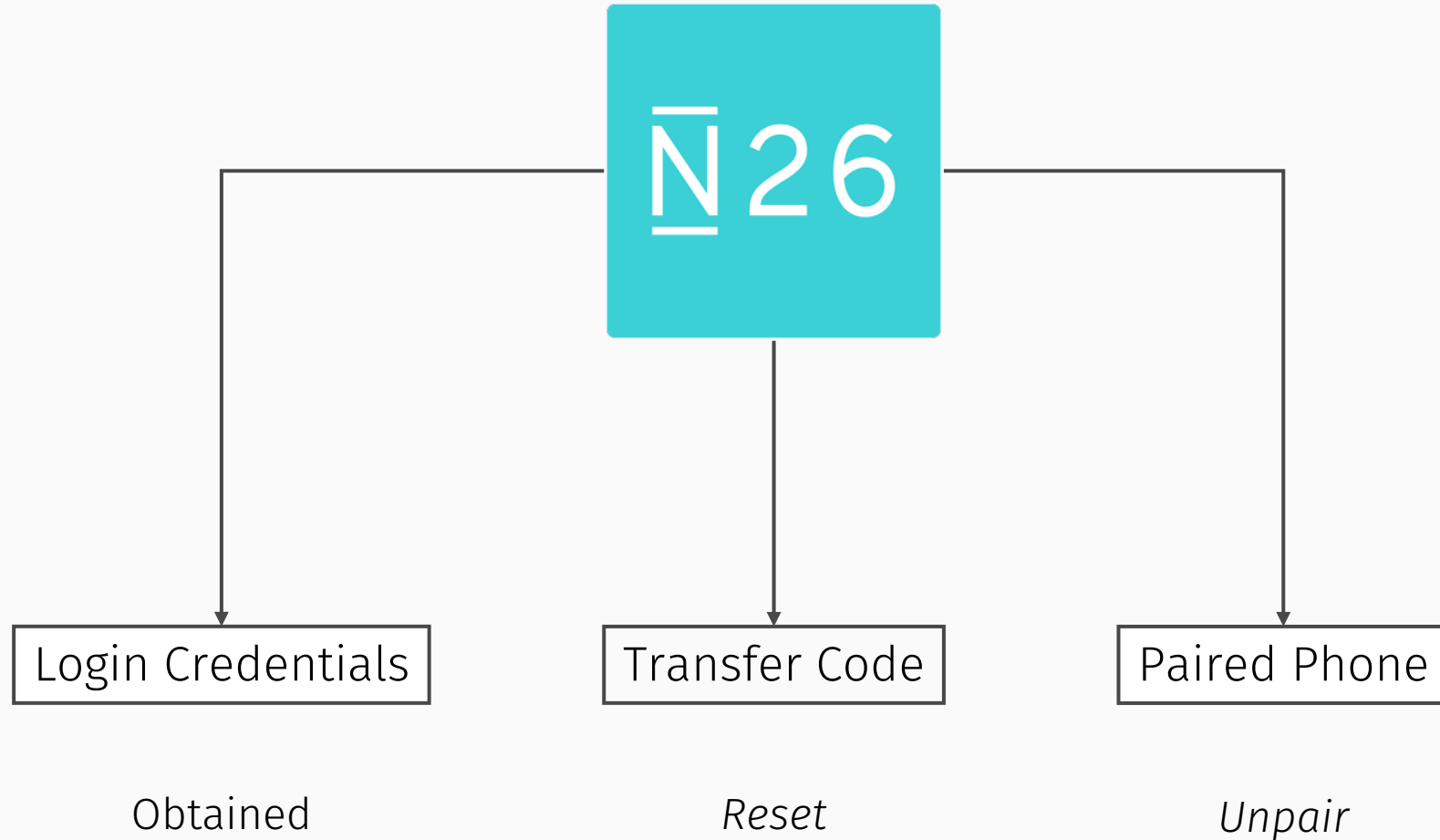




# Account Hijacking

— Transfer Code & Paired Phone—

# Account Hijacking



# Unpair

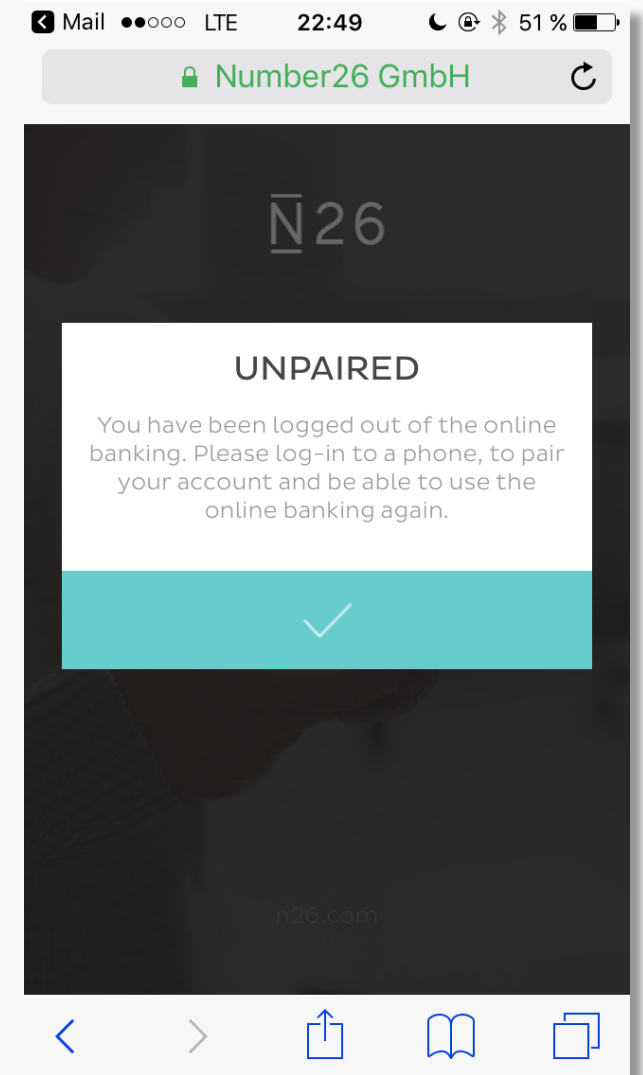
1. Start unpairing
2. Follow link in unpairing email
3. Enter transfer code
4. Enter MasterCard ID
5. Receive token via SMS
6. Done

Email account

Transfer Code

MasterCard

SIM Card



How N26 Made a Mistake in Every Step

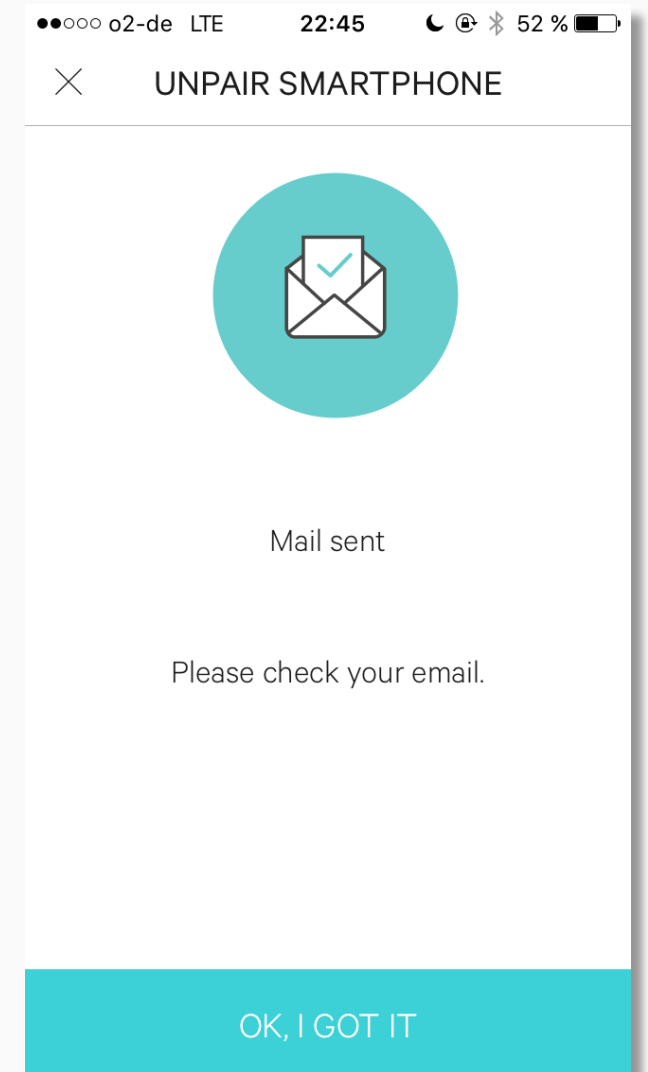
# Unpair: Email

GET <https://api.tech26.de/api/unpair/upstart>

Response:

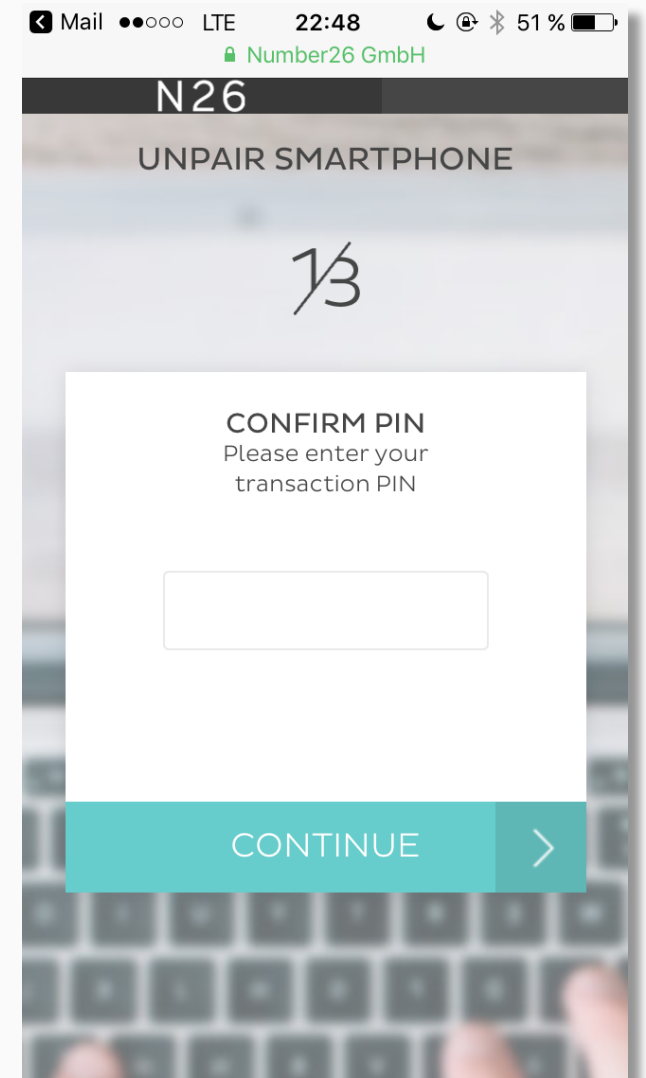
```
{
  "date": "09/13/2016 19:54:38.586",
  "message": "https://my.number26.de/unpair/4a4e9088-351f-4521-84a5-44602741176d",
  "success": true
}
```

Unpairing link is also sent as response!



# Unpair: Transfer Code

We will get right to this!

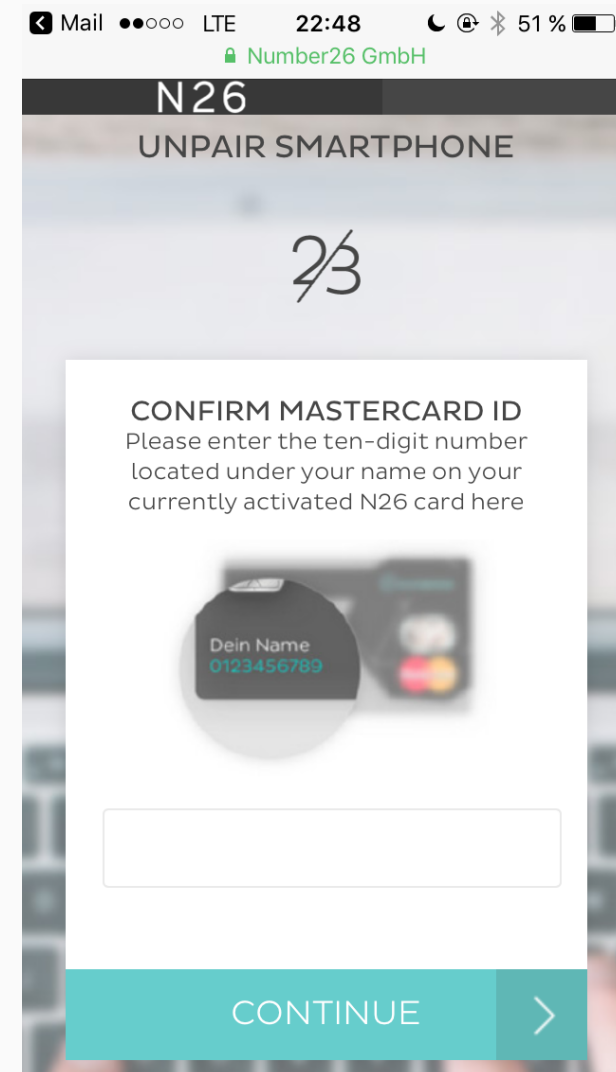


# Unpair: MasterCard ID

- MasterCard ID is printed on the card
- However, each transaction contains the following:

```
{  
  "amount": -0.11,  
  "cardId": "b8484ca2-a674-4f1c-afd1-896a3bfe6d15",  
  "linkId": "0123456789-372287",  
  "merchantCity": "DUESSELDORF",  
  "merchantCountry": 0,  
}
```

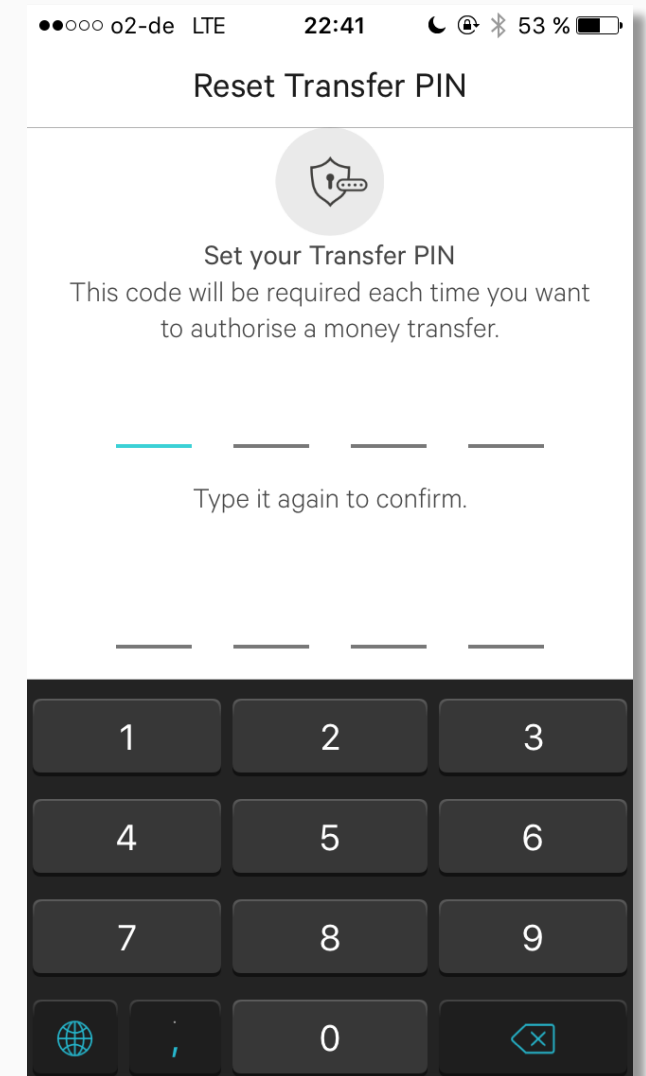
MasterCard ID is part of every MasterCard transaction!



# Unpair: Transfer Code

- The transfer code is unknown
- Changing it, however, does not require the old transfer code:
  1. Enter MasterCard ID
  2. Choose and confirm new transfer code

The transfer code can be changed by only knowing the MasterCard ID!

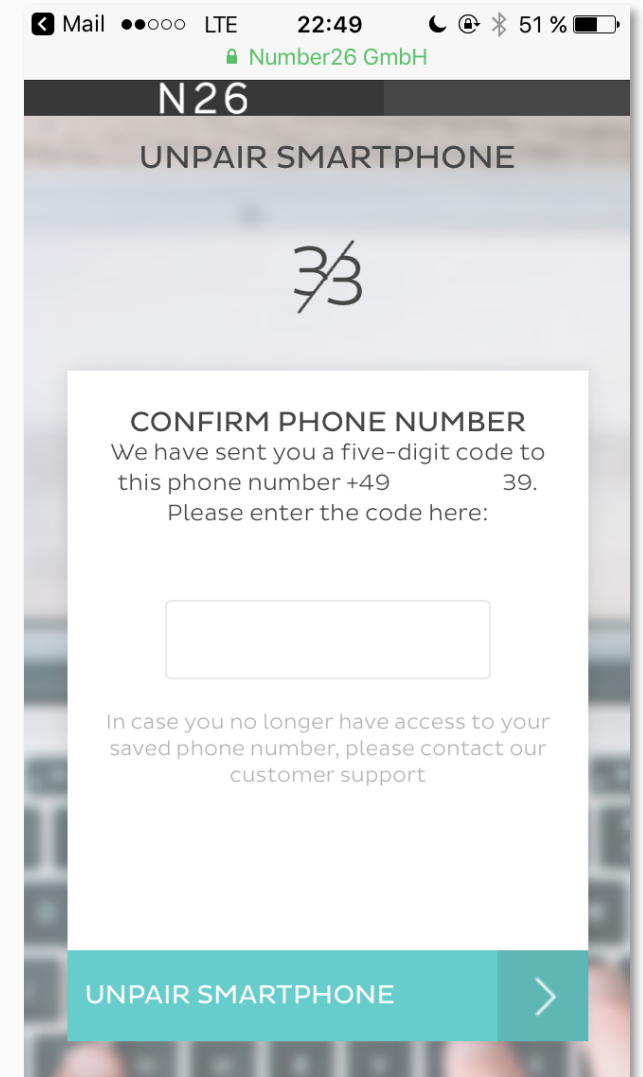




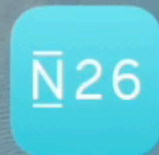
# Unpair: SMS

- SIM card is inaccessible
- Token sent to the phone number has
  - 5 digits
  - Numbers
- Only 100.000 possibilities
- No brute force protection at all
  - 160 requests/sec
  - Takes 5 min on average

The SMS token can be determined through brute force!



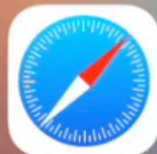
Demo



N26



Phone



Safari



Mail



Threema

Calling the Support

# Calling the Support

- The customer support is the most powerful entity in the N26 security model
- Certain things can only be changed by the support
  - Email address
  - Name
- They can also unpair your phone
- Customer authentication:
  1. MasterCard ID
  2. Current account balance
  3. Place of birth



# Calling the Support: Place of Birth

GET <https://api.tech26.de/api/me?full=true>

```
"userInfo": {  
  "birthPlace": "Schlaraffenland",  
  "email": "vincent.hauptert@gmail.com",  
  "gender": "MALE",  
  "firstName": "Vincent",  
  "lastName": "Hauptert",  
  "nationality": "DEU",  
  ...  
}
```

All required information for customer authentication are available!

User receives no notifications of any chances!



*“I only got €50 on my account,  
why should I care?”*

# Stealing Money you don't have

- Many accounts might have a low credit balance
  - Inactive
  - Not using N26 seriously, e. g., as salary account
- N26 offers an instant overdraft
  - Granted in 2 minutes
  - Between €50 and €2000
  - Requires paired device

With access to the paired device, the attacker can steal money beyond the actual balance!





# Disclosure & Conclusion

- Responsible Disclosure
  - All issues have been reported to N26 on September 25, 2016
  - CCC reached out to N26
- Professional contact and reaction
- Incremental fixes
  - Time of first fix unknown
  - Last fix on December 13, 2016
  - Apparently, all issues are resolved

## N26 has to assign a higher priority to security

- Releasing videos with the caption “Mobile First Meets Safety First” and claiming security is of “paramount importance” is not enough
- FinTechs squander the trust in financial institutions
- Authorities need to take a closer look at the security of banks



Thank you!