Secure payments in times of cybercrime and social engineering

Frankfurt am Main | 10. November 2016
## Agenda

1. Introduction
2. From crime in paper-based transactions to cybercrime
3. Examples of "industrialised cybercrime" in private banking
4. Social Engineering: cybercrime in the corporate banking business starts with employees
5. How can you as a company protect yourself and what to do in the event of fraud?
6. Contact details of Commerzbank
7. Disclaimer
There has always been fraud in payment transactions. But what has changed with digitalisation?

› A signature is easily copied. A good forgery might pass a visual check in daily business.
› In fraud in paper-based payment transactions the criminal fakes the customer’s identity.

The digital signature:

30460221009e0339f72c793a89e664a8a932d 
f073962a3f84eda0bd9e02084a6a9567f75aa 
022100bd9cbaca2e5ec195751efdfac164b76 
250b1e21302e51ca86dd7ebd7020cdc0601

› A digital signature cannot be “imitated” by technical means.
› Criminals attempt to get the customer to initiate the fraudulent payment procedure themselves or they get the customer to let them have access to their system.
Fraud with SEPA corporate client direct debits (B2B)

The fraud path:

1. The underlying transaction

2. Presentation of the mandate

3. Confirmation of the entry

4. Presentation of the B2B direct debit

5. The non-cancellable collection
Agenda

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>From crime in paper-based transactions to cybercrime</td>
</tr>
<tr>
<td>3</td>
<td><strong>Examples of &quot;industrialised cybercrime&quot; in private banking</strong></td>
</tr>
<tr>
<td>4</td>
<td>Social Engineering: cybercrime in the corporate banking business starts with employees</td>
</tr>
<tr>
<td>5</td>
<td>How can you as a company protect yourself and what to do in the event of fraud?</td>
</tr>
<tr>
<td>6</td>
<td>Contact details of Commerzbank</td>
</tr>
<tr>
<td>7</td>
<td>Disclaimer</td>
</tr>
</tbody>
</table>
How malware gets on your computer

Paypal: Confirmation of a payment?

- E-mail attachments, usb sticks, drive-by exploit kits and links in e-mails are the most common methods of malware contamination of computers used to confirm a fake payment to the debit of your Paypal account.

- In the example on the left, a link to query the transaction is included in the e-mail - contrary to a genuine Paypal payment.

- A look at where this link really leads to shows, depending on the program, that the e-mail is not from Paypal.

- In this case, a click on the query link would start a php script.

- Don't click anything in this email. Open a plain browser on your computer and go to Paypal.

- Enter your login details and check if the transaction has effectively been made.
Example from private banking
Multi-TAN Trojan: here 100 TAN Trojan
Example from private banking
Multi-TAN Trojan: here 100 TAN Trojan
Reverse transfer Trojan
The fraud starts with a message about an erroneous payment received.
Return to classic phishing as a “predicate offence”. Mails and websites only rarely have spelling mistakes.
# Agenda

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>From crime in paper-based transactions to cybercrime</td>
</tr>
<tr>
<td>3</td>
<td>Examples of &quot;industrialised cybercrime&quot; in private banking</td>
</tr>
<tr>
<td>4</td>
<td><strong>Social Engineering: cybercrime in the corporate banking business starts with employees</strong></td>
</tr>
<tr>
<td>5</td>
<td>How can you as a company protect yourself and what to do in the event of fraud?</td>
</tr>
<tr>
<td>6</td>
<td>Contact details of Commerzbank</td>
</tr>
<tr>
<td>7</td>
<td>Disclaimer</td>
</tr>
</tbody>
</table>
In contrast, cybercrime in companies starts with employees, because corporate banking is essentially more complex.

- Various products for electronic banking
- Major national differences in the technologies used and authorisation media
- The payment transaction products used in Germany have a high level of technical security

**Conclusion**

Fraud schemes that have been practised abroad for years have found their way into the German-speaking countries.

In their attacks, criminals aim specifically to deceive a company's employee in order to ...

... induce him/her to initiate seemingly legal payments.

... gain access to the employee’s workplace computer to initiate payments themselves, for example, using remote access.
Fraud scenarios in practice: social engineering + remote access tools

This scam is similar to the “Microsoft technician” variant, but here a call is received purportedly from the bank itself. The caller pretends that technical support has to be provided for a necessary update.

In fact, however, the supposed “software update” installs a “remote access tool”, which is otherwise useful support software employed for requested technical assistance. To distract the user's attention away from the installation, he is sent to various computers to enter the login and authorization details.

Specific cases are known from the UK and France – but apparently this method is also widely used in other countries.
Fraud scenarios in practice: Forged confirmations of payment

› A new business partner wants to order goods. Because he is unknown to your company, he agrees to pay before delivery.

› The goods are produced for the customer.

› Shortly before the delivery date, the recipient submits a purportedly genuine payment voucher, bank statement or Swift message to confirm that the payment was effected and now expects delivery of the goods.

› The scammer insists on urgent delivery of the goods stating that non-delivery is considered a breach of contract. The payment confirmations were forged, mostly including all details of the remitter.

› Stamps on payment vouchers are no evidence. Only the credit entry to your bank account is what counts.
Fraud scenarios in practice: Forged cheques (overpaid invoices)

› Previously: For the booking of a holiday home, payment by cheque is requested. The cheque is then issued for an amount that is too high and you are asked to re-transfer the excess amount claimed to be "accidentally" overpaid.

› New: In corporate banking, the check is sent to the bank directly in a letter. The letter contains instructions to credit the check specifying the address and account number.

- Case 1: Previously, the company received an order with a much lower value. Subsequently, the excessive payment is stated to be a mistake. A re-transfer is requested.

- Case 2: The company receives an e-mail purportedly from the "transferring" bank. The “bank” requests that the erroneous payment be re-transferred, but specifies a third recipient account.

› The cheques are fake or not covered.
Fraud scenarios in practice: invoice fraud

- False invoices for imaginary services that may indeed match the content and service of an expected invoice. The competent persons in the company are first located via social media research.

- The invoice can come by e-mail or post. Real vendors’ stationery is also used in part.

- Sometimes, the employee immediately receives a (last) reminder, followed by a call to put him under pressure. Here too, official signatures of the managers (e.g. from balance sheets) are quite often added to fake orders presented as the basis of the invoice.

- For large amounts, invoice fraud is not as easy to commit due to companies’ internal control measures for new debtors or changed bank details of debtors.
Fraud scenarios in practice: invoice fraud

- It's also known as little CEO-Fraud. An invoice which the boss has supposedly received and which he now passes on to you as an accountant for payment. The amount is usually just below 10,000 EUR. The boss does not need any reply.

---

Rechnung

<table>
<thead>
<tr>
<th>Rechnungs-Nr.</th>
<th>2010-10-155</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Anzahlung Webentwicklung: 20.000,00 EUR</td>
</tr>
</tbody>
</table>

Gemäß § 19 UStG enthält der Rechnungsbetrag keine Umsatzsteuer. Ich bitte den Betrag sofort auf das folgende Konto zu bezahlen.

Kontoinhaber:
Ralf Neddermeyer
IBAN: DE57 7002 2200 0073 0199 44
BIC: FDBDEDEMXXX
Fraud scenarios in practice: mandate fraud

- E-mail or letter purportedly from a supplier with alleged corrections to bank details. The information usually immediately follows a genuine e-mail from a real sender for an expected invoice, after the business partner's mail server has been hacked. There are also cases where the change of bank details is advised to real business partners well in advance by post!

- In one case, this was even done as a large-scale mailing to all business partners of the company, so that the Treasurer himself finally believed that the company probably had a new bank account which he did not know. Possible receipt channels are e-mail, fax, letter on correct letterhead stationery etc.

- Mostly larger amounts (5 to 8 figure amounts are known). The target countries of these fraud schemes are often in South East Asia.
Fraud scenarios in practice: mandate fraud

The account confirmation issued regularly by the bank has been used as a template to inform the company’s business partner about an allegedly new banking connection. The company used the same confirmation letter beforehand.

The signatures are those of the bank’s employees.

The letter matches the bank’s letter.

Commerzbank was replaced by INVEST BANK (visible in the interruption of the signature).

This method of fraud is particularly well-known in industries where credit transfers are made on the basis of delivery notes OR as a follow-up on intercepted e-mails including an invoice.
Fraud scenarios in practice: man in the middle

- Business partners communicate by e-mail from time to time to arrange a deal, without noticing that other similar e-mail addresses have slipped in over time. Since the content basically corresponds to the original, no suspicion arises. It is only when the invoice is issued that the bank details of the invoice are manipulated!
- The fraud is only recognized on receipt of a reminder or when the goods are not received by the payer.
- Mostly larger amounts (5 to 8 figure amounts are known).
- The target countries of these fraud schemes are mostly in Europe, China, Hong Kong or South East Asia.
Fraud scenarios in practice: man in the middle with guarantees
Fraud scenarios in practice: man in the middle with cheques.
Fraud scenarios in practice: CEO/CFO fraud targets the helpfulness of employees and the trust in your relationship bank

1. The purported CEO/CFO entrusts the employee with a task requesting absolute confidentiality. He is to inform a third party (counsel, consultancy, law office) of all required details by e-mail.

2. The employee is then contacted by such third person, subtly reassured and manipulated. The fraudster's goal is to get further information (limits, authorisations, required signatures).

3. The employee is instructed to initiate a payment, also using signatures already effected that he previously disclosed to be required (distributed signature). In this process, he is subtly included in the e-mail correspondence between the purported CEO and the third person.

4. The employee known and familiar to us as a bank initiates the payment with all due urgency. Queries are normally not answered due to confidentiality.
Fraud scenarios in practice: CEO/CFO fraud targets the helpfulness of employees and the trust in your relationship bank

5. Problems are clarified with the purported CEO/CFO. Signatures not authorised, for instance, are now to be authorised on the basis of the commercial register.

6. The fraudsters use counterfeit documents, ID cards, certifications and BaFin documents. They exploit the employee of a company inciting him to put the bank under pressure by claiming that the payment is urgent.

7. Requested assurances and confirmations are provided.

8. If the credit balance in the account is insufficient, the employee is sent to the bank to request an overdraft. A balancing of the account is promised for the next day via funds allegedly to be provided by the parent company or the subsidiary. If no overdraft is granted, the fraudster contents himself also with smaller amounts.
Fraud scenarios in practice: spear phishing ("CFO fraud"/"CEO fraud")

› A forged, seemingly internal e-mail instructs an employee to carry out a transaction. The instruction mostly comes from the management in these cases and announces a call, for example, by a responsible lawyer.

› One of many known schemes to deceive an employee is a pending merger, which is strictly confidential due to the stock exchange listing of that employee’s company.

› Specific cases are known from the UK, the USA and Germany.
Fraud scenarios in practice: spear phishing ("CFO/CEO fraud")

The e-mail is followed by the announced call. The simulation of whole telephone and video conferences is known to us too. The telephone number in the display can be falsified via "spoofing".

- Any documents requested are usually also delivered as falsifications (copies of identity cards, merger agreements, etc.).
- The fraud is repeated by phone calls from a safe distance until the employee at the company notices the deception.
- In the case of payments to Asian countries, the instructions are often initiated after 12 noon CET, with same-day value demanded in most cases.

Practical example no. 1: According to the employee, the CFO of their own holding company called personally, and the employee thought he had recognised his voice. The audit department was called in and was on the spot when more phone calls from the fraudster followed. The similarity of the CFO's voice was confirmed.

Practical example no. 2: The treasurer at a newly acquired company receives a phone call from an alleged board member. He too thought he had recognised the board member's voice, since he had called him just three weeks previously to congratulate him on his company anniversary. Both were bogus calls.
Fraud scenarios in practice: impacts of a CEO fraud

EANS-Adhoc: FACC AG / FACC AG - Victim of cybercriminal activities

19/01/2016 | Adhoc
ad-hoc disclosure transmitted by euro adhoc with the aim of a Europe-wide distribution. The issuer is solely responsible for the content of this announcement.

19.01.2016

Today, it became evident that FACC AG has become a victim of a crime act using communication- an information technologies. The management board has immediately involved the Austrian Criminal Investigation Department and engaged a forensic investigation. The correct amount of damage is under review. The damage can amount to roughly EUR 50 million. The cyberattack activities were executed from outside of the company.

EANS-Adhoc: FACC AG / UPDATE: FACC AG - Cyber-Fraud

29/01/2016 | Adhoc
ad-hoc disclosure transmitted by euro adhoc with the aim of a Europe-wide distribution. The issuer is solely responsible for the content of this announcement.

29.01.2016

On January 19, 2016 FACC AG announced that it became a victim of fraudulent activities involving communication- an information technologies. To the current state of the forensic and criminal investigations, the financial accounting department of FACC Operations GmbH was the target of cyber fraud. FACC's IT infrastructure, data security, IP rights as well as the operational business of the group are not affected by the criminal activities. The damage is an outflow of approx. EUR 50 mio of liquid funds. The management board has taken immediate structural measures and is evaluating damages and insurance claims. All production- and engineering units operate in an unaffected and normal way. An economic threat to the company concerning liquidity does not exist. The management board will decide on further actions after the outcome of the forensic investigations is available. FACC AG will announce its Q1 results tomorrow, as scheduled.

Source: facc.com
Fraud scenarios in practice: impacts of a CEO fraud

EANS-Adhoc: FACC AG / Chief Financial Officer Mandate Terminated. Reorganisation of Financial Department

Board of Directors (Appointments and Changes)

23.02.2016 | Adhoc
FACC AG announces that the mandate of Mr. Minten Gu as chief financial officer of FACC AG terminates with immediate effect. The Supervisory Board initiated the search for a successor. To the current state of the forensic and criminal investigations, the criminal activities which targeted the financial accounting department were fraudulent actions involving the use of a false identity (so-called fake president fraud). FACC's IT infrastructure, data security, IP rights as well as the operational business of the group are not affected by the criminal activities. No evidence of malice has been identified. The management board is fundamentally reorganizing the financial department and pursuing damages and insurance claims. To assist the management board in the reorganization of the finance department, the supervisory board appointed its member, Mr. Yongsheng Wang, on an interim basis to the management board.

EANS-Adhoc: FACC Operations GmbH / FACC Operations GmbH strengthens the balance sheet

20.02.2016 | Adhoc
ad-hoc disclosure transmitted by euro adhoc with the aim of a Europe-wide distribution. The issuer is solely responsible for the content of this announcement.

Capital measures
20.02.2016

The supervisory board of FACC AG today approved a resolution to authorize an increase of the equity of its subsidiary company FACC Operations GmbH through a capital increase of its parent company FACC AG. This capital measure is done by a capital increase of FACC Operations GmbH from FACC AG in the amount of EUR 47 mil. and a capital contribution of FACC AG in favor of FACC Operations GmbH in the total amount of EUR 79 mil. in form of an irrevocable debt waiver of a shareholder loan. This measure will significantly strengthen the equity position of FACC Operations GmbH. This company is also the issuer of a bond and a promissory note loan. The transaction will have no influence on the balance sheet of FACC AG GROUP.
Fraud scenarios in practice: blackmail (at present hypothetical)

› Possible scenario: An employee has his personal information, e.g. on Xing, and is requested as a contact via headhunters or consultants with a false identity. By confirming, he exposes his network and his position, if they are not already visible to everyone.

› If the employee's name in privately used social media is the same – and his private information is visible to everyone, or he accepts “friend requests” from personally unknown people – and he is linked to his own children and their posts about where they do sports regularly – all this together creates high potential for blackmail!

› So far, this is more of a hypothetical scenario

› Some social media provider:
How malware finds its way onto your Computer ransomware / Crypto Trojan

- E-mails with attachments, mostly including a kind of script to install the malware.
- Very often in use on e-mails to Human Resources, hidden in attachments of an online application.
- Ransomware can be inactive for a couple of days.
- Even if you pay Bitcoins to get the crypto key, there is no guarantee the key will work at all or that all files can be rescued.
- If you think you have fallen victim to ransomware, switch your computer off. (Keep On/Off pressed until the computer is switched off).
- Operating systems should be up to date.
- Anti-virus programmes should be installed and updated as well as a firewall.
- Use programmes that recognize crypto-Trojan actions/ patterns and prevent attacks
- Backups should not be permanently connected.
# Agenda

1. Introduction
2. From crime in paper-based transactions to cybercrime
3. Examples of "industrialised cybercrime" in private banking
4. Social Engineering: cybercrime in the corporate banking business starts with employees
5. **How can you as a company protect yourself and what to do in the event of fraud?**
6. Contact details of Commerzbank
7. Disclaimer
How can companies protect themselves?

› Train your staff on these fraud schemes. Awareness is the best protection for your company.
› Ensure IT security in your company (operating system, firewall, anti-virus software, user rights, updates and changes of start passwords also for the telephone system). Never install software that third parties force on you on an unsolicited basis.
› Never open e-mails from unknown senders. Do not open e-mail attachments, which you do not trust. Application documents should only be opened on a stand-alone computer that is not connected to your network.
› Identify processes subject to risk and ensure checks are made.
  – Not only payment inputs or payment releases are security critical.
  – Changes to master data (account details/ delivery addresses) should be secured by queries (also for salary payments)
  – Checking back in case of doubt: Call a known contact or supervisor in your company, at the bank or your business partner to prevent fraud.
› Train your staff on the risks of social media if contact requests from unknown persons are easily accepted. Create awareness that when a person divulges information in social media he should always consider how this information can be used against himself.
› Check all surprising circumstances with common sense.

› Do employees in your company have a single signature authority?
› Can employees sign with unlimited authorization in the name of your company?
› Has your company provided a fax or e-mail undertaking for orders to the bank?
› Have you instructed your bank to block paper-based payment orders?
› Are publicly known signatures also used to authorize bank orders?
What to do, when it went wrong?

What should you do if you become a victim?
› Contact your bank immediately, especially if the payment is still “fresh”.

– Payments are guaranteed to be returned only if they have not been credited to the beneficiary’s account.

– Payments may also still be returned under certain circumstances, if the money has not been withdrawn from this account (goodwill).

› A credit transfer can only be successfully recalled if this is done promptly.

› Even if you were able to prevent a fraud attempt, please advise us of the beneficiary’s account details.

› Please clarify with your management if you want to report a fraud case or attempted fraud to the police – which we would suggest you to do.

What can Commerzbank do for you in the worst case?
› Recall the credit transfer promptly.

› Use its fine global network of international banks.

› We can make contact with the investigating authorities specialised in cybercrime and business crime throughout Germany.

› We can recommend further steps, depending on the amount, country and circumstances involved.
Conclusion

Cybercrime in the corporate banking business is not as “industrialised” as in browser-based banking. A high level of diversity makes writing malware “too expensive”.

Attacks are mostly made via social engineering.

Training employees, good process steps, checking “strange” circumstances with common sense and checking back with known contacts through a different channel (telephone) help prevent such fraud.

Any loss due to detecting fraud too late may possibly be averted even after the money has left your account, if you do not hesitate to inform your bank so a recall of the credit transfer can be initiated.
Commerzbank AG

Commerzbank AG
GS-OS IS Security Consulting & Research
MSB CTS & FI, Product Management Cash Services,
Fraud prevention

e-mail: msb.fraudmanagement@commerzbank.com

Postal address:
60261 Frankfurt/Main
Tel.: +49 69 136-20
Mail: info@commerzbank.com
Disclaimer

This presentation was prepared and drawn up by Commerzbank AG. Its publication is intended for professional and institutional clients.

All information in this presentation is based on sources considered to be reliable. Commerzbank AG and/or its subsidiaries and/or branches (described here as the Commerzbank Group) cannot, however, assume any guarantee or warranty with respect to the accuracy of the data.

The assumptions and evaluations included here reflect our best assessment at the current point in time. These can be amended at any time without notice. This presentation is exclusively for information purposes. It is not intended to be and is also not to be perceived as an offer or commitment to buy or sell any equities or bonds that are mentioned in this presentation.

The Commerzbank Group may use the information from the presentation for its clients even before publication. The Commerzbank Group or its employees may also own, buy or at any time sell equities, bonds and corresponding derivatives if they consider this to be appropriate. The Commerzbank Group shall not assume any responsibility or liability for any kind of expenses, losses or damage that are connected with the use of any part of this presentation in any manner.