Secure use of your ING Corporate Card

Introduction

You can use your ING Corporate Card to pay for such things as hotel bookings, conferences, flight tickets, restaurants and taxis. But your Corporate Card offers much more.

For instance, travel agencies use the Corporate Card for the convenience it offers for reservations. People are increasingly using the Card because it is an easy and secure way of making payments and business payments.

Of course, you would like to be certain that your payments are processed correctly. You can find more information about this in this document. ING is working hard to make paying secure, now and in the future. But we can't do this alone. Stick to our basic rules to stop criminals in their tracks.

These basic rules are explained in this brochure. We give tips on how to make secure payments and recognise fraud. We also explain what we as ING are doing to ensure that using your Corporate Card stays as secure as possible. There's also a glossary at the end with an explanation of the internet and other terms used in this brochure.

Handy and free

Use the ING Commercial Card app and the ING Commercial Card portal. This enables you to retain an overview of your transactions, statements, total payments, balance and remaining limit. You can find the ING Commercial Card app in the Apple App Store and in Google Play (Android).
To find the app, enter: ING Commercial Card app
You can find the ING Commercial Card portal at: www.ingcommercialcard.com

Report fraud immediately

If you have you become a victim of fraud with your Corporate Card, you should report this to us immediately. This will enable us to help you and other customers, now and in the future. We are available for you 24 hours a day, 7 days a week from home or abroad and also via our local access numbers. You can find these at the end of this brochure.

Contents

1. Five basic rules for secure payment

We have translated the uniform security rules for banking in the Netherlands into five basic rules for using your Corporate Card. This makes it easy for you to remember.

Basic rule 1: Protect your codes

You don't give your door key to a random passer-by. So don't do this with your security codes. Keep these safe and secure.

- **Remember your codes**
  For security codes/passwords, don't select date of birth, name of a family member or another code that is easy to guess. Are you afraid that you will forget your codes? Then why not make a note of them in such a way that they cannot be decoded or try to devise a mnemonic. A sentence with capitals and digits is secure and easy to remember. For example: 'Prefer U2 to Beethoven's 6th!'. If using a whole sentence doesn't fit, use the first letters of each word: 'LU2dd6evB!'

- One way to remember the PIN code of your Corporate Card is to select a word for each digit in the PIN code, with the number of letters being equal to the digit. You can then use the 4 words to make a sentence. If your PIN code is: 9246. Your sentence could then be: Edinburgh (9) is (2) very (4) lovely (6).

- **Don't allow anyone to watch**
  Don't allow anyone to watch while you're entering your codes. Ways of doing this include screening the number pad with your body or with your free hand.

- **Never give out your codes**
  If someone asks for your security codes or passwords, for example for the Commercial Card portal, never give these out. Your codes are strictly personal. You should never tell anyone and remember that ING employees will never ask for your security codes: not at the reception desk, not by telephone, not by email, not via another non-ING website or app and also not in any other way.

Basic rule 2: Safeguard your Corporate Card

You don't throw your wallet around. So don't do that with your Corporate Card. Safeguard it well.

- **Be careful with your Corporate Card**
  Your Corporate Card is strictly personal. So don't lend it to anyone. Don't leave your Corporate Card lying anywhere and store it in the same secure place immediately after use. Make sure that nobody can take your Corporate Card without you realising it.

  Don't hand your Corporate Card to a waiter, but go to the payment terminal yourself. If it is actually necessary to hand over your Corporate Card, check that you receive the same card back.

  Check at least once a day whether you still have your Corporate Card. This is mandatory and is also stated in our conditions.

- **Don’t be distracted**
  Don’t be distracted when you’re using your Corporate Card. If you’re not careful, your Corporate Card can easily be changed, for example for a credit card of the same colour. We call this the quick-change routine. If you suspect that it is not secure to use it, follow your gut feeling and keep your Corporate Card somewhere safe.

- **Check regularly that you still have your Corporate Card**
  If you are addressed on the street by a random person or someone bumps into you, always check that you still have your Corporate Card. If you don’t get it back after you’ve used it for payment, contact us immediately (24 hours a day, 7 days a week) on +31 (0)10 428 95 81 or via one of our local access numbers (you can find these at the end of the brochure).

Basic rule 3: Secure your devices

You always lock your front door. Do the same to the devices you use to carry out internet transactions with your Corporate Card, such as your smartphone, tablet, desktop and laptop. Make sure these are secure. Don’t give criminals the opportunity to install malicious software and such things as a ‘trojan’ to obtain your personal details including your Corporate Card details.

- **Install only legal and known software**
  Make sure that your smartphone is setup so that apps from unknown sources are not permitted. So don’t ‘root’ or ‘jailbreak’ your smartphone and only download apps from official app stores. Install only legal software from a source that you have checked. You can do this by going to the provider’s official website. If you are offered an unknown software program, don’t download it immediately but first check it using your virus scanner software.

- **Use the latest app and operating system versions**
  Both the Commercial Card app as well as your smartphone, tablet and computer operating systems are regularly updated with more and better security technologies. That’s why you should update regularly. Preferably set updates to download automatically.

- **Use an access code for your devices**
  An access code prevents others gaining very easy access to your personal data. This doesn’t only include your Corporate Card details, but also your contacts, messages and photos.

- **Use a virus scanner, firewall and anti-spyware**
  To make internet payments with your Corporate Card, only use a desktop or laptop that has a virus scanner, firewall and anti-spyware. This gives viruses and unsolicited programs less chance. These days, there are also virus scanners to offer additional protection to smartphones and tablets.

- **Secure your wireless internet connection (WiFi)**
  Without a secure internet connection, you should not carry out any internet transactions using your Corporate Card. That is why you should secure your own WiFi with a password. Your internet provider can help you in this. If you use a public WiFi network outside the home, you should preferably not carry out any internet transactions with your Corporate Card.

Basic rule 4: Check your payments and statements

It is always good to check carefully exactly what you are paying before you pay. And also to check regularly what was debited. You can do this via the ING Commercial Card portal or using the Commercial Card app. This app also displays your transactions real-time.

- **Know what you pay**
  Check whether the amount that you have to pay has been shown on the display or - if you are abroad and need to sign the receipt - that the correct amount is stated on this. Save the copy of the receipt for your own administration. This means you will always have proof if the amount on your Corporate Card statement later proves to be incorrect.

Ensure that the amount in a foreign currency doesn't surprise you later if this is recalculated to the amount for which you are charged on your Corporate Card.

- **Stick to the correct order**
  For internet purchases, only enter your details, such as credit card number, expiry date and security codes, if you are certain of your purchase.

- **Check your online statements**
  Check your statements at least once every two weeks. You can then assess whether transactions are legitimate and can inform us immediately of any misuse.

- **Report loss in time**
  If you suffer loss because you have been unable to check your Corporate Card statements for some time, we may ask you to demonstrate this. Loss that is reported more than thirty days after the date of your statement will in principle not be compensated.

Basic rule 5: If in doubt, call ING

If you know for sure or you suspect that you are a victim of fraud, let us know immediately. By contacting us, we can take immediate measures to prevent further loss. For example, we will have fake websites removed from the internet so that other customers are not affected by fraud.

- **Call immediately**
  If you suspect fraud, you can call us immediately. Even if your Corporate Card, Commercial Card app or ING Commercial Card portal User-ID is blocked. Also call us if you receive a suspect email or if someone has tried to obtain your Corporate Card details.

- **Make sure that we can contact you**
  In the event of suspect transactions, we would like to be able to contact you quickly by telephone or SMS. So please make sure that you forward your mobile number to our customer services. You can do this via +31 (0)10 428 9581 or via our local access numbers (you can find these at the end of this brochure).

2. Recognise fraud

In spite of all the security measures and your careful use, there is still a risk of your Corporate Card being misused. The information below will help you to recognise the various attempts to do this.

Fraud via your Corporate Card

- **Skimming**
  A known form of fraud is skimming; copying the credit card details that are on your card's magnetic stripe. In recent years, various measures have been taken to prevent skimming. This means that this form of fraud is less prevalent.

- **Theft, exchange tricks and distraction manoeuvres**
  Your Corporate Cards can still be exchanged or stolen and your security codes watched while you enter them. People are also still distracted at cash dispensers, enabling criminals to escape with the cash they've just taken out. The ten euro trick is an example of this. You will be distracted by a 10 euro note on the ground while criminals take your cash from the cash dispenser.

  This form of fraud occurs mostly in shops or at cash dispensers. Prying eyes stand over your shoulder watching while you enter your PIN code and criminals try to distract you in various ways.

Fraud via your computer

- **Phishing**
  In fraud via phishing, criminals fish for your security codes using SMS or email, or via a fake website. You receive an SMS or email requesting that you click on a link. Without realising, you arrive on a fake website, for example from the ING Commercial Card portal, where you are asked to log in using your security codes. You should never click on suspect links but should delete the email immediately from your mailbox.

  Phishing messages can be recognised as follows:
  - The message usually includes an urgent reason for action.
  - You will be asked to click on a link. Without realising, you arrive on a fake website where you are asked to log in using your security codes.
  - The message often seems to be from your bank.

- **Malware**
  Malware is malicious software used by criminals for such things as remote operation of your computer. They can use this to obtain your login details. Malware can be installed easily on a computer without anti-virus software and a good firewall. This often happens without you realising it. A familiar example of malicious software is a trojan.

  Malware can be recognised as follows:
  - Sometimes, internet pages don't quite look the same as you are used to. For example, there is an extra entry field for your telephone number.
  - A computer infected by malware is slower and freezes more often.

Fraud by telephone

- **Phishing**

  Criminals also use telephone phishing during a telephone conversation to fish for your security codes, such as your Corporate Card PIN code, your ING Commercial Card portal login details or other personal data. Phishing can also be done via SMS, email and fake websites.

  On the telephone, criminals often appear to be someone else. They may act as though they are an ING employee or computer or software company employee. They tell a believable story to which you usually need to respond immediately. They will then ask for your security codes. Remember that ING employees (or those from other companies) will never ask for your security codes.

  If you're unsure as to whether you have an ING employee on the telephone, ask for his or her name and call us back using the number at the end of this brochure. An ING employee will understand this. We will then connect you with this employee.

  Examples of fake telephone calls:
  - Several days after entering your credit card details in a phishing email, your bank will call, informing you that there is something wrong with your Corporate Card. If you follow the directions by providing a few final additional details to 'resolve the problem', you will notice later on your statement that your Corporate Card has been used fraudulently.
  - You are contacted by someone who acts as though they are a computer or software company employee. The employee asks you to go to a website to install software.
  - He or she will often state that this is necessary for your computer's security. The software you are asked to install is malware. If you install this, data you later enter for an internet transaction with your Corporate Card will be vulnerable!
  - A person acts as though he or she is an ING employee and says that he/she needs to verify your details. For example, your username and password for the ING Commercial Card portal.
  - ING employees will never ask for this. So never hand out your codes.

3. What does ING do?

We have already given a lot of advice and tips on secure payment. Of course, ING also uses various invisible and visible technologies to keep the use of your Corporate Card secure.

Security on the Corporate Card

- The chip on your Corporate Card and the anti-skimming device on the card entry slot of a cash dispenser prevent skimming.
- If you pay using a Corporate Card, these days, you are usually asked for your PIN code rather than your signature. This is more secure.
- As well as your Corporate Card credit card number, the card also has a CVC (Card Validation Code) on the reverse. This three-digit code provides an additional check.

Security during payment

- **SMS Security Alert**
  During high-risk transactions in which additional verification is desirable, you will receive a Security Alert via SMS a few seconds after the transaction. This SMS will ask you to confirm the transaction. Should something be incorrect, you can report this to us immediately and your credit card can be blocked quickly to prevent further misuse. The SMS will be sent from number: +44 78 60 04 74 44.
  - If it concerns a known purchase, respond in the way as indicated in the SMS. No further action is then required of you.
  - If it concerns an unknown purchase, respond in the way as indicated in the SMS. ING will block your Corporate Card immediately and will send you a second SMS with additional information on how you should proceed further.

  This service is free for every Corporate Card customer. The only thing that we need from you is your correct mobile number. Call our customer service to be certain that we have your correct number.

  It is good to know that responding to the Security SMS has no liability consequences in the event of fraud. Your purchase will just be processed. Depending on the situation, your card can be blocked temporarily or permanently for subsequent purchases.

- **Mastercard ID check**
  Internet purchases at companies that participate in Mastercard ID check receive background protection against misuse. You will then see a screen with the text ‘Processing’. In most cases, ING carries out all security checks in the background, but for some transactions, we will ask you to enter a one-off code. You will receive this code by SMS. Make it easy for yourself and us and make sure that we have your mobile phone number.

- **Blocking the Card**
  In the event of suspect situations, ING can decide to block your Corporate Card preventatively. You will always be informed about this as quickly as possible by telephone, SMS or letter. Should you notice that your transaction didn’t go through, please contact us immediately.

4. Fraud, what now?

ING does everything to prevent you becoming a victim of fraud. And if you try to follow the advice and tips in the brochure as closely as possible, criminals will have little opportunity to commit fraud with your Corporate Card. If you nevertheless become a victim of fraud, we will resolve this as quickly as possible for you. That is why you should act as follows:

Report fraud

- **As quickly as possible**
  Report fraud or a suspicion of fraud to us by telephone as quickly as possible. You can do this 24 hours a day, 7 days a week. In any event, do this no later than 30 days after the date of your statement (digital or paper version). If you report this quickly, we can usually prevent that the amount is collected from you or from the company. This prevents unforeseen financial consequences for you or the company. We can also send you a new Corporate Card immediately.

- **Fraud form**
  Following the telephone report, we will send you a fraud form by regular mail, or if you prefer, by email. Our condition: return the form to us within 14 days. The faster the forms are completed and returned, the sooner your fraud report can be processed. We may sometimes need extra information from you if the shopkeeper of the shop where the misuse has taken place demands this.

- **Report**
  If your Corporate Card is used fraudulently while lost, stolen, not received by you or not requested by you, you must attach a police report to your fraud form.

Compensation

- **Our policy**
  If you are not to blame, fraud is always compensated. During the telephone conversation, our employee will do everything possible to ensure that you are not charged for this. In some cases (for instance if the collection order has already been sent by us), we can, however, not prevent this. We will always consult with you regarding the situation so that the compensation is arranged as quickly as possible.

  The compensation will be finalised using your written statement and our investigation into the misuse of your Corporate Card. We will always inform you in writing.

5. Glossary

A

Anti-skimming device

An anti-skimming device is a device on a cash dispenser’s card entry slot. This prevents criminals from using a card reader to copy credit card data. Copying credit card data is known as skimming. The anti-skimming devices can differ per cash dispenser. The cash dispenser screen will display the correct entry slot.

Anti-spyware

Anti-spyware is one of the tools that you can use to protect your computer. This software ensures that no unsolicited programs can be installed that can spread your personal data.

Anti-virus software

See ‘Virus scanner’

B

Botnet

A botnet is a network of very many computers, which is infected by a Trojan or virus. This turns the computer into a kind of robot that can operate independently and automatically. The infected computers can be anywhere. Your computer can also be part of this. Criminals can then assign a task to all these computers in one go. The computers are then used, for example, to send phishing emails. Or to intercept your Corporate Card details.

Browser

A browser is a computer program with which you can view internet websites. Well-known browsers are Internet Explorer, Chrome, Firefox and Safari.

C

Commercial Card portal

With the ING Commercial Card portal you can view your Corporate Card statements digitally for the past 12 months. You can download the statements at a digital location requested by you. This means you don’t need to archive paper versions.

Computer virus

See ‘Virus’

Cookie

A cookie is a small file that is placed on your computer by a website. This saves your surfing behaviour. Many webshops use cookies so that your data are already entered the next time you visit.

Commercial Card app

The Commercial Card app is the official app for your Corporate Card. You can use this to view transactions for the past 12 months. Search for ‘ING Commercial Card app’ download in the Apple App Store or in Google Play (Android).

CVC

CVC stands for Card Validation Code. It is a 3-figure security code that appears on the reverse of your Corporate Card immediately after your signature. You may be asked for this if you make internet payments with your Corporate Card.

Cyber crime

Cyber crime is criminality via internet. Criminals send emails in which they ask for your login details and/or credit card details (phishing) and create websites that look very much like ING websites. They also try to obtain your personal details from your computer via a virus that they send with another program (a so-called Trojan).

D

Detection

Detection is the tracking of suspect actions. ING has a team of in-house experts involved daily with payment security. We continuously analyse suspect transactions and operations. And we take action where necessary. ING works closely with police, government and other parties, nationally and internationally. This enables us to inform you quickly and in the best way possible.

DdoS attack

During a DdoS attack, an internet site is bombarded with data traffic. This undesired data traffic is obstructed by the firewall. Once the undesired data traffic is too big, the firewall becomes so busy obstructing this undesired traffic that the desired visitors can no longer get through. ING uses extremely high level security measures. These measures are designed to separate undesired data traffic from good data traffic.

E

EMV chip

The EMV chip has been the chip on your Corporate Card for a number of years. This enables you to pay in shops using your Corporate Card and PIN code. The EMV chip is an international standard that is used across the world. The chip reduces credit card fraud in shops. You no longer swipe your Corporate Card along a magnetic stripe card reader, but insert your Corporate Card in the payment terminal. The EMV chip is read in this way.

Extension

An extension is an extra application for your browser that you can download yourself. This makes it possible to add new functions to your browser. Examples of an extension are Adobe Reader for reading PDF files and Flash for watching YouTube videos.

F

False email

See ‘Phishing’

Firewall

A firewall is one of the tools that you can use to protect your computer. This software helps you prevent others gaining access to your computer when it is connected to the internet or a computer network. A firewall checks incoming and outgoing internet traffic. You will receive an alert in the event of dubious data exchange.

Fraud

You can become a victim of fraud in various ways. This brochure has been formulated to inform you about fraud.

I

Identity fraud

Identity fraud means that criminals can collect your personal and financial details and later misuse these. Instilled habits, such as innocently throwing away financial information, Corporate Card statements, a signature or copy of your proof of identity, can facilitate identity fraud. But criminals can also obtain personal details via phishing and social engineering. A criminal can then use your name to submit a request for a credit card.

Internet criminal

Internet criminals are involved with criminal activities on the internet. They send emails in which they ask for your login details and/or credit card details (phishing). Internet criminals also make websites that look very much like ING's website. Or they try to obtain your personal details from your computer via a virus that they send with another program (see Trojan).

J

Jailbreaking

Jailbreaking is circumventing a security measure from an iPhone, iPod touch or iPad operating system. By jailbreaking the device, the user can install such things as apps that are not approved by Apple. This makes such devices more vulnerable to viruses and malware.

M

Malware

Malware is a collective name for malicious and/or harmful software. The word is a combination of the English 'malicious software'. Malware is designed specially to infiltrate your computer without you necessarily being aware of this. Malware can for example enter your computer via email or images on websites.

MasterCard ID check

See chapter 'What does ING do?'

Money mule

A money mule makes his or her bank account available for criminal activities. Criminals deposit money in the bank account, channel it through to other accounts, or take it out in cash. They do this to hide stolen money from the police and the law.

N

NCSC

Dutch National Cyber Security Centre; a collaboration of governments and companies. Mission: NSCS contributes to jointly improving Dutch society's digital resilience, and with this offers a secure, open and stable information society by delivering insight and offering an operating perspective.

O

Operating system

A computer, tablet or smartphone can only function if it has software on it. Software that is written to allow such devices to function is called an operating system.

P

Password
Secure banking needs a strong password. A password is strong if it is not easy to guess and is difficult to hack. Use a strong password for all your online environments.

Phishing
Phishing is ‘fishing’ for personal data by criminals. With one goal: obtaining information about your Corporate Card and using it to carry out transactions. They can do this by email, telephone or website. You will, for example, be asked to click on a link in a fake email. The message will look misleadingly like an ING email. You will then be transferred to a fake website on which you enter your Corporate Card details. Without you noticing, criminals can now carry out transactions with your Corporate Card.

Preventative blocking
To keep payment traffic secure, ING takes immediate measures in suspect situations. To protect your Corporate Card, we may proceed to preventative blocking, for example, if we suspect that your Corporate Card has been skimmed. We will then block your credit card and try to contact you immediately.

R

Ransomware
Ransomware is a blackmail method that uses malware. Ransomware is a program that blocks your computer and then demands money to ‘release’ the computer again. Payments (for example made with your Corporate Card) don’t result in your computer being ‘released’ because the criminals are only after your money.

Rooting
Rooting is circumventing a security measure from an Android smartphone or Android tablet operating system. By rooting the device, the user can install such things as apps that are not approved for the Android Market. This makes such devices more vulnerable to viruses and malware.

S

Security Alert Service
See chapter ‘What does ING do?’

Security expert
We have a team of in-house security experts that continuously analyses suspect transactions and actions. We take action where necessary. ING works closely with police, government and parties such as the Dutch Association of Banks.

Skimming
Skimming is copying your Corporate Card details by placing an extra card reader on a cash dispenser’s card entry slot. Criminals can then copy your personal PIN code, after which, they can use the skimmed data to take out cash. By placing a special device on cash dispenser card entry slots, ING aims to prevent criminals from using card readers. Shopkeepers are also periodically encouraged to check whether criminals have possibly manipulated their payment terminals.

Smishing
Smishing is phishing by SMS. See ‘Phishing’

Social engineering
Criminals use social engineering to extract confidential information from you. They misuse human traits such as curiosity, trust, greed, fear and ignorance. Social engineering appears in many forms, from false websites to phishing emails and from telephone conversations to personal contacts at the door. Criminals get you to carry out certain actions, such as entering personal details, security codes or credit card details, clicking on a button or installing malware.

Spyware
Spyware is software that is installed on your computer without you knowing. This can be used to collect details about the user and send this to third parties.

T

Ten euro trick
Criminals try to distract someone who is about to take cash from the cash machine by throwing a ten euro note on the floor. They tell you that you dropped the note but in the meantime, steal your cash from the cash machine.

Access code
You can set a code on your computer or smartphone/tablet/computer so that others cannot simply use your device.

Trojan (or Trojan horse)
Trojan is derived from the Trojan horse. A Trojan is a program ‘disguised’ as an innocent file that is installed on your computer without you knowing. This enables criminals to access your computer remotely without you realising this. They can use Trojans to obtain such things as your username and password for the Commercial Card portal.

V

Virus
A virus is a harmful form of software. Viruses can cause serious damage to your computer through which you lose (confidential) information. Criminals can also use a virus to watch your computer and obtain your user name and password.

Virus scanner
A virus scanner is one of the tools that you can use to protect your computer. This software checks whether your computer contains viruses and can remove these viruses.

W

WiFi
WiFi is the English abbreviation for a wireless network. You can access the internet via a wireless network.

Worm
A worm tries to spread itself across networks. A worm replicates itself automatically, like in a chain reaction. Mostly, this happens via email addresses that are found on an infected computer.

6. Important telephone numbers

In the event of fraud or suspected fraud, you can contact us 24 hours a day, 7 days a week on

+31 (0)10 428 95 81

or via our local access numbers. You can find these numbers on:

www.ingwb.com/cardcontact

Don’t hesitate, we’re here for you!

ING Bank N.V. has its registered office at Bijlmerplein 888, 1102 MG Amsterdam, the Netherlands, commercial register no. 33031431 in Amsterdam. ING Bank N.V. is registered with De Nederlandsche Bank (DNB) and the Financial Markets Authority (AFM) in the Credit Institutions and Financial Institutions Register. ING Bank N.V. is also subject to the supervision of the Authority for Consumers & Markets (ACM). For more information regarding the supervision of ING Bank N.V., please contact DNB (www.dnb.nl), the AFM (www.afm.nl) or the ACM (www.acm.nl).

In the context of this publication 'ING' and 'bank' are understood to mean: 'ING Bank N.V.'

ING