OCBC

Mari Bertransaksi dengan Aman & Nyaman

Edukasi Keamanan Kartu Nasabah 2024

Terus bersama,
melaju jauh

Daftar Isi

Kenali Jenis Transaksi *Merchant Offline*

Deep Swipe Card

Transaksi ini yang paling lazim dilakukan. Caranya adalah Anda menyerahkan Kartu Debit atau Kartu Kredit kepada *merchant* untuk digesekkan pada mesin EDC kemudian masukkan PIN.

Cardless & Contactless Payment

Untuk melakukan transaksi *contactless,* pemegang kartu harus membawa dan menempelkan kartu pada mesin EDC *contactless.* Atau bisa melalui *generate token* pada aplikasi *mobile banking* nasabah.

QR Payment

Transaksi ini dilakukan dengan cara *scan QR code* melalui aplikasi OCBC mobile. Biasanya ada *merchant* yang menggunakan QR dinamis dimana nominal sudah auto terisi sesuai transaksi dan tipe statis di mana kita mengisi sendiri nominal transaksinya. Anda harus berhati-hati agar tidak salah memasukkan nominalnya sebelum akhirnya kita memasukkan PIN dan membayar.

Kenali Jenis Kejahatan Transaksi *Merchant Offline*

Counterfeit

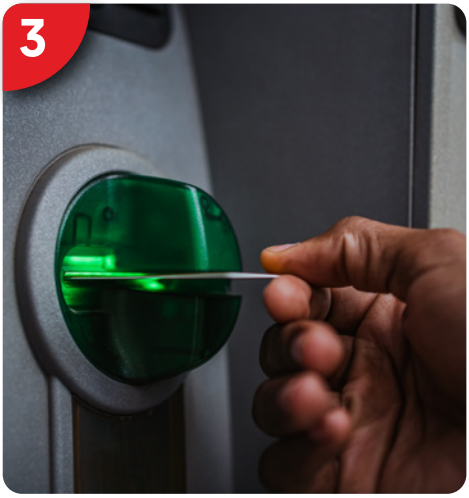
Counterfeit ini adalah membuat replika atau tiruan kartu debit/kartu kredit dengan cara *"skimming"* data yang ada dalam *magnetic stripe.* Setelah direplika penjahat tersebut akan menggunakan informasi tersebut untuk melakukan transaksi, dan transaksi tersebut akan masuk ke dalam tagihan nasabah.

Lost & Stolen Cards

Kejahatan ini terjadi jika kartu debit atau kartu kredit kita hilang, dan ditemukan oleh orang aayang tidak bertanggung jawab. Karena itu, jika kartu Anda hilang sebaiknya lekas melakukan pemblokiran.

ATM Skimming

Hampir mirip dengan *counterfeit*, ATM *skimming* ini adalah kejahatan dengan mereplika atau menduplikasi info privasi yang terdapat dalam kartu ATM Anda. Hal ini biasanya terjadi pada saat kartu digesekkan ke mesin EDC.



Merchant Double Swiping

Double swiping adalah tindakan *merchant* melakukan gesekan kedua kartu pembayaran untuk memperoleh otorisasi dari penerbit kartu. Umumnya, gesekan kedua tidak terkait dengan otorisasi atau penyelesaian tetapi digunakan untuk membuat catatan sekunder untuk mendukung akuntansi, pelaporan, atau program hubungan pelanggan. Hal ini seharusnya tidak boleh, karena jika memang untuk kebutuhan *customer relation* maka *merchant* bisa eksplore dari integrasi data mesin EDC dan POS-nya (*cash register system*). Karenanya, selalu waspada atau ajukan keberatan jika *merchant* melakukan *double swiping*.

Kenali Jenis Transaksi *Online*

Transaksi *Online* dengan Kartu Debit

- Biasanya digunakan untuk bertransaksi di *e-commerce*, termasuk hiburan berlangganan (Netflix, Spotify, dan sebagainya).
- Saat bertransaksi Anda akan melakukan verifikasi transaksi melalui OTP *(One Time Password)* yang dikirim ke ponsel Anda.
- Khusus di bank OCBC, transaksi *online* bisa dilakukan dengan menggunakan Kartu Debit OCBC *Online*.

Transaksi *Online* dengan Kartu Kredit

- Biasanya juga digunakan untuk bertransaksi di *e-commerce*, termasuk hiburan berlangganan (Netflix, Spotify, dan sebagainya).
- Ada dua jenis transaksi *online*, yang satu dilengkapi dengan keamanan berupa OTP *(One Time Password)* yang dikirimkan ke ponsel Anda. Yang satu lagi, tidak dilengkapi fitur keamanan berupa OTP dan ditentukan oleh pihak merchant (bukan pihak bank).

Kenali Jenis Kejahatan Transaksi *Online*

Phising

Phishing adalah pembuatan replika pesan email/halaman web untuk mengelabui pengguna dengan tujuan mengirimkan data pribadi, keuangan, atau kata sandi.

Email ini sering kali meminta informasi seperti pulsa, nomor kartu, informasi rekening bank dan kata sandi yang akan digunakan untuk melakukan transaksi yang tidak sah. Karena itu, selalu waspada jika ada email yang mencurigakan dan meminta data privasi, amati lebih jeli alamat email pengirim, jika ragu tidak ada salahnya menghubungi *contact center* resmi.

Hacking

Penjahat semakin canggih dan paham teknologi, mereka mampu meretas ke dalam sistem untuk mendapatkan akses ke data pelanggan untuk untuk melakukan transaksi tanpa kartu atau dengan membuat *counterfeit*.

Electronic Pickpocketing

Hal ini terjadi ketika penjahat menggunakan pemindai untuk mencuri informasi dari *contactless* kartu tanpa sepengetahuan nasabah. Ada baiknya untuk menggunakan penutup atau pelindung kartu/paspor saat tidak digunakan.

Kasus *Trending* Kejahatan Transaksi *Online*

Trend Quishing

Ternyata dengan maraknya pembayaran menggunakan metode QRIS, mulai muncul potensi kejahatan transaksi dengan QRIS, yaitu: *Quishing* atau *QR Code Phishing*. Penipu menggunakan *QR code* palsu untuk mengelabui korban untuk memperoleh informasi pribadi atau mengarahkan ke situs web berbahaya.

Skenario yang biasa digunakan biasanya sebagai berikut:

1. Pelaku mengirimkan pesan teks, email, atau melalui media sosial dan meminta korban untuk memindai *QR code* palsu dengan alasan untuk mendapatkan hadiah/*voucher/cashback* sebagai bagian dari sebuah promo.
2. Setelah dipindai, akan diarahkan ke situs web palsu dan diminta informasi pribadi.

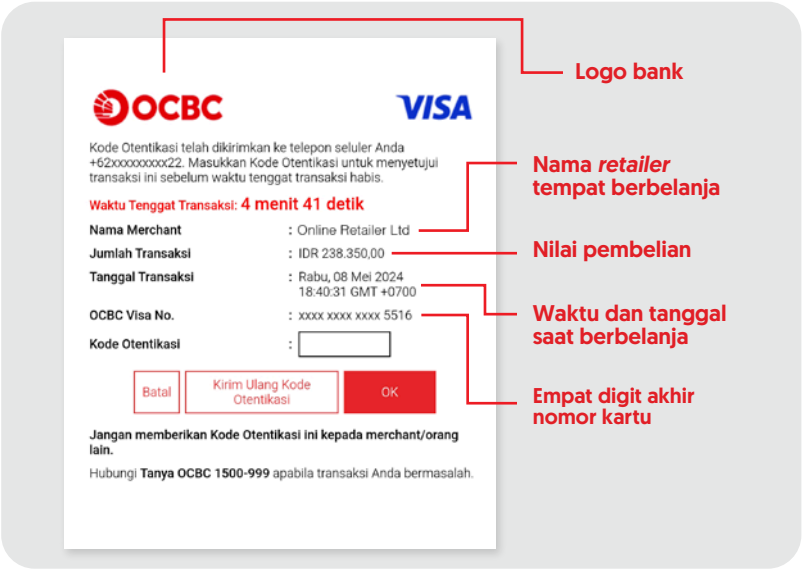
Cara Terhindar dari *Quishing*

1. Verifikasi *QR code.*
2. Hanya pindai *QR code* dari sumber terpercaya. Pastikan terdapat nama atau identitas yang tertera pada aplikasi sesuai dengan tujuan pembayaran yang diinginkan.
3. Cek keaslian *website.*
4. *QR code* mengarahkan kita website tertentu. Pastikan URL mengarah ke situs web resmi. Juga cek link pada *QR code* apakah diawali dengan https:// karena hanya URL tersebut yang aman.
5. Belanja/transaksi di *official account.*
6. Pastikan hanya melakukan pembelian/pembayaran melalui toko resmi/*official account* dan gunakan aplikasi pembayaran resmi dari penyedia layanan yang terpercaya. Kita juga dapat cek testimoni pelanggan lainnya untuk memastikan kredibilitas toko dan keaslian barang tersebut.
7. Tenang saat bertransaksi.
8. Jangan terburu-buru untuk menyelesaikan pembayaran. Pastikan setiap langkah pembayaran benar, jangan sampai terjebak oleh penipu.
9. Lakukan autentikasi dua faktor.
10. Autentikasi dua faktor tiap *account* membantu dalam melindungi *account* yang kamu miliki. Jangan lupa *log out* dari perangkat jika sudah tidak digunakan lagi.
11. Jangan bagikan data pribadi.
12. Hindari memberikan informasi pribadi seperti Nomor Kartu Debit/Kredit, CVV, *expired date, password,* PIN, dan kode OTP.
13. Laporkan aktivitas mencurigakan.
14. Jika ada yang mencurigakan segera hubungi TANYA OCBC 1500999/+62 21-26506300 (dari luar negeri), email ke tanya@ocbc.id, WhatsApp Bisnis OCBC 0812-1500-999

Kenali Jenis-Jenis *Merchant*

Merchant Secure

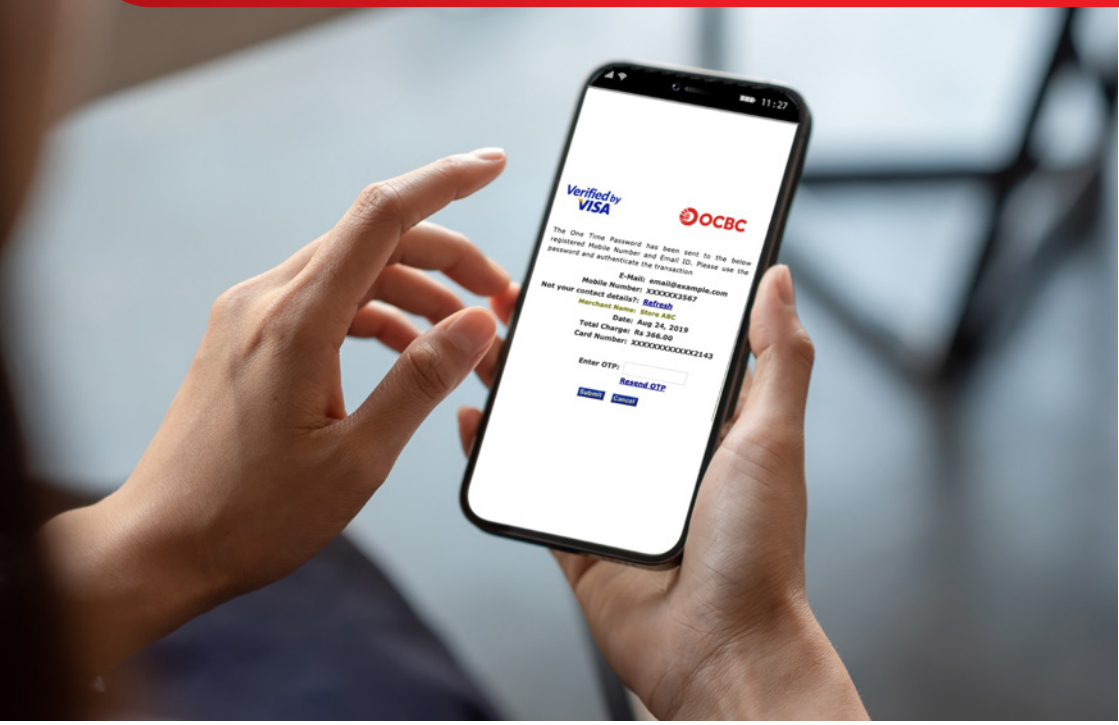
- *Merchant secure* adalah *merchant* yang memiliki sistem pembayaran yang aman dan dapat dipercaya karena memiliki sistem keamanan yang kuat dan efektif untuk melindungi informasi privasi dan sensitif pelanggan.
- *Merchant secure* ini biasanya memiliki keterangan "*Verified by VISA*" atau "*Verified by Mastercard*" atau penyedia sistem pembayarannya (contoh lain: JCB dan American Express).
- *Merchant secure* ini juga menerapkan standar keamanan PCI DSS (*Payment Card Data Security Standard*).
- *Merchant* tipe ini biasanya juga dilengkapi dengan system 3DS yaitu: *Three Domain Secure* (3D-Secure atau 3DS) adalah protokol keamanan transaksi online untuk melakukan konfirmasi (biasa disebut autentikasi) terhadap pemegang kartu dengan cara mengirimkan *one time password* (OTP).



Merchant Unsecure

Nasabah diharapkan berhati-hati ketika bertransaksi di tipe *Merchant Unsecure* karena rentan terhadap serangan *cyber* dan pencurian data. *Merchant* tipe ini tidak mematuhi standar keamanan industri PCI DSS (Payment Card Data Security Standard) yang sudah disebutkan tadi. Pastikan Anda bertransaksi di *verified merchant* ya.

Kenali Jenis Keamanan Transaksi *Online*



Transaksi *Secure* dengan OTP

Transaksi secure dengan OTP (*One Time Password*) adalah transaksi keuangan yang dilengkapi dengan lapisan keamanan tambahan berupa kode yang hanya dapat digunakan sekali dan biasanya dikirimkan ke perangkat yang telah terdaftar, seperti ponsel, ataupun email nasabah.

Nasabah harus memasukkan OTP yang diterima untuk autentikasi transaksi yang berlangsung. Setelah OTP diverifikasi, transaksi akan diproses dan dana akan ditransfer dari akun pelanggan ke akun *merchant*.

Perlu diingat untuk TIDAK memberikan informasi terkait OTP kepada pihak manapun. Karena OTP bersifat rahasia dan hanya Anda yang boleh mengetahuinya.

Transaksi *Secure* Tanpa OTP

Transaksi *secure* tanpa OTP ini mengacu pada transaksi keuangan yang tetap aman dan terlindungi meskipun tidak menggunakan OTP.

Transaksi ini aman jika *merchant* tersebut menerapkan sistem keamanan yang kuat & memadai seperti:

- Memiliki enkripsi data.
- Memiliki verifikasi identitas (3DS atau 2FA/verifikasi dua faktor).
- Pemantauan transaksi.
- Mengikuti ketentuan PCI DSS untuk memastikan sistem pembayaran memenuhi persyaratan yang ketat.
- Pembaruan keamanan, dimana sistem dan perangkat lunak selalu diperbarui dengan *patch* keamanan terbaru untuk mengatasi kerentanan yang diketahui.

Transaksi ini sangat bergantung pada jenis *merchant*-nya, maka pilihlah bertransaksi di *merchant secure* ya, yang sudah diverifikasi oleh penyedia sistem pembayarannya.

Transaksi *Unsecure* (Transaksi Tanpa OTP)

Transaksi *unsecure* adalah transaksi yang terjadi tanpa adanya lapisan keamanan tambahan 3DS (*Three Domain Secure*) ataupun OTP.

Transaksi tipe ini rentan terhadap peretasan data privasi dan data sensitif pemegang kartu, risikonya antara lain kejahatan transaksi yang sudah dijelaskan di awal tadi.

Untuk mengurangi risiko ini, bertransaksilah di *merchant secure* yang sudah dilengkapi dengan multi-layer keamanan.

Tips Menjaga Keamanan Rekening

Saat Penerimaan Kartu Debit/Kartu Kredit

1. Segera tandatangani kartu Anda di panel yang disediakan setelah kartu diterima.
2. Jangan pernah menuliskan PIN Anda, tapi diingat.
3. Pastikan kartu selalu dalam pengawasan Anda.
4. Catat nomor rekening kartu kredit Anda dan nomor telepon untuk melaporkan kartu yang hilang atau dicuri. Simpan catatan tersebut di tempat yang aman kalau perlu menggunakan *password*.
5. Saat membuat PIN, selalu hindari yang mudah ditebak misalkan: nama, nomor telepon, tanggal lahir, atau kombinasi ketiganya.
6. Jangan pernah mengungkapkan PIN Anda kepada siapa pun. Bahkan lembaga keuangan, polisi, atau pedagang tidak boleh meminta PIN Anda. Karena Anda adalah satu-satunya orang yang boleh tahu.

Tips Bertransaksi Aman & Nyaman

1. Bertransaksi di Secure Merchant.
   Perhatikan *merchant* di tempat Anda bertransaksi apakah ada keterangan "*Verified by VISA*" atau pun penyedia system pembayarannya misalkan: Mastercard, JCB, dan American Express).
2. Gunakan *web browser* yang aman.
3. Gunakan jaringan internet yang aman untuk melakukan perbandingan antar toko.
4. Lindungi kerahasiaan data sensitif kartu AndaJangan bagikan informasi privasi Anda termasuk Password, PIN, CVV dan OTP.
5. Ketahui siapa yang memiliki akses ke kartu Anda. Jika kartu kredit Anda dipinjam oleh anggota keluarga (pasangan, anak, orang tua), dengan atau tanpa sepengetahuan Anda, Anda mungkin bertanggung jawab atas pembelian/penarikan tunai mereka.
6. Cek kebijakan pengiriman & pengembalian barang.
7. Jangan pernah kirimkan informasi pembayaran via email.
8. Simpan dan catat transaksi Anda.
9. Review dan cek *Billing Statement* Anda secara rutin.

Tips Menjaga Kerahasiaan OTP & CVV

1. Selalu waspada dan teliti.
2. Jika ada nomor asing yang menghubungi dan mengaku sebagai petugas Bank, perlu berhati-hati. Pastikan kembali Anda dihubungi oleh akun dan nomor resmi Bank OCBC melalui:
   - TANYA OCBC: 1500-999/ +62 21-26506300 (dari luar negeri
   - Akun WhatsApp tanda verified dengan centang hijau
   - Email Resmi OCBC dan dengan domain/akhiran @ocbc.id
3. Waspada penipuan minta kode OTP & CVV.
   Modus penipuan yang mengatasnamakan Bank suka memberikan informasi palsu. Seperti pengkinian data, konfirmasi transaksi, atau iming-iming hadiah. Biasanya Nasabah akan dikirimkan link atau pesan singkat meminta data rahasia. Hati-hati! Jangan berikan kode OTP kepada siapapun termasuk petugas Bank.
4. Rutin mengganti *password* dan PIN.
   Ganti *password* dan PIN mobile banking Anda secara berkala. Gunakan kombinasi angka yang unik dan berbeda tiap diganti. Hindari PIN atau *password* yang mudah ditebak seperti tanggal lahir, alamat rumah, nomor berurutan, dan lain-lain.
5. Gunakan koneksi internet yang aman saat bertransaksi.
   Koneksi internet yang tidak aman juga bisa menyebabkan kebocoran kode OTP. Seperti menggunakan wifi tanpa pengaman di tempat umum, menjadi sasaran empuk bagi *hacker* untuk mengakses perangkat dan mencuri data rahasia. Hindari mengakses mobile/*internet banking* dengan akses internet umum.
6. Blokir kartu dan aplikasi.
   Apabila Anda terlanjur membocorkan kode OTP & CVV kepada orang lain atau pihak yang dicurigai sebagai penipu, segera laporkan ke TANYA OCBC di 1500999 dan minta lakukan pemblokiran kartu dan aplikasi agar data rahasia Anda tidak disalahgunakan.
7. Jangan lupa untuk laporkan segala tindak mencurigakan dan penemuan penipuan kode OTP adi TANYA OCBC di 1500999.
   Selalu waspada dan jaga data rahasia Anda! Informasi lebih lanjut: Digital Security | OCBC

Appendix

Tren *Cashless Overview*

Indonesia sudah mulai mencanangkan Gerakan Nasional Non Tunai (GNNT) sejak tahun 2014 dengan wacana Indonesia Menuju *Cashless Society* pun mulai bermunculan.

Namun, *shifting* besar mulai terlihat di tahun 2020 ketika Pandemi Covid-19 muncul dan juga munculnya Bank Digital.

Kini, kita bisa melihat perubahan dari penggunaan *cash* menjadi digital

Aktivitas belanja online sebelum COVID-19

9% berbelanja kebutuhan sehari - hari secara online

Aktivitas belanja online setelah wabah COVID-19

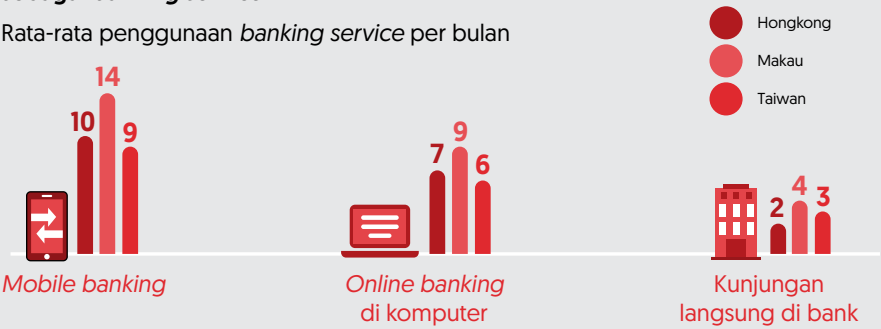
63% berbelanja kebutuhan secara online/melalui telepon daripada saat sebelum peraturan *social distancing*

86% lanjut untuk berbelanja online/melalui telepon ketika peraturan *social distancing* berlaku

Sumber: Three steps to make a cashless world work: PWC

Mobile dan _online_ banking sudah menjadi cara yang umum digunakan _customer_ sebagai _banking service_

Rata-rata penggunaan _banking service_ per bulan



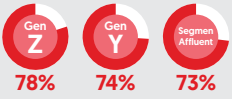
Perubahan ini pun berdampak pada penggunaan *Digital Banking.*

Berdasarkan VISA *Consumer Payment Attitude* 2.0, penggunaan *Mobile & Online Banking* menjadi cara utama nasabah mengakses kebutuhan perbankan, di mana melalui *mobile banking* ini pun turut mendukung pertumbuhan transaksi digital.

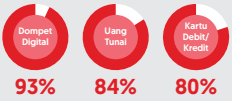
Berdasarkan Visa Consumer Payment Attitudes Study 2022

2 dari **3**
Masyarakat Indonesia sudah mencoba untuk go cashless.

Diantara mereka, generasi muda yang menjadi pendorongnya.



Pilihan memakai dompet digital telah melampaui pilihan membayar dengan uang tunai.



1 dari **3**
Konsumen Indonesia telah pernah menggunakan kartu *contactless* terutama GenY dan segmen affluent

Tingkat penggunaan, kesadaran, dan minat terhadap kartu *contactless* semakin meningkat.

Berdasarkan data dari VISA tahun 2022, Masyarakat Indonesia sudah mulai meninggalkan uang tunai, mulai memilih untuk go digital dalam hal bertransaksi.

Kenali Detail Kartu Anda

Chip

Mungkin Anda telah menyadari banyak merchant yang memilih untuk memasukkan kartu Anda ke chip terminal daripada menggesek untuk transaksi. Itu adalah hal yang bagus karena microchip yang ada di dalam kartu Anda tidak bisa diduplikasi.

Proses encryption yang kuat menghindari akses yang tidak diinginkan ke informasi yang ada dalam microchip, membuat pembayaran elektronik ini lebih aman.

Garis Magnetis

Garis magnetis dikodekan dengan nomor kartu, tanggal kedaluwarsa, dan informasi lainnya.

Signature Panel

Berada di belakang kartu Visa dengan desain tamper evident yang merupakan fitur personifikasi yang menyesuaikan dengan kartu Anda.
Jika ada seseorang yang berusaha menghapus tanda tangan Anda, nantinya akan terlihat tulisan "VOID"

Nomor Kartu

Nomor kartu yang tertera di kartu Anda selalu dimulai dengan nomor "4". Nomor kartu harus berjajar dengan lurus.
Pada kartu yang palsu, nomor akan terlihat kabur sehingga Anda tidak bisa melihat jelas nomor kartu Anda.

Hologram Burung Merpati

Lambang burung merpati dari Visa harus muncul secara tiga dimensi dan bisa bergerak saat kartu dimiringkan.
Banyak kartu palsu yang hanya memiliki gambar satu dimensi di sticker foil.

Card Verification Value

Card Verification Value (CVV) adalah tiga digit kode yang ada di belakang kartu Visa Anda. Ketika Anda berbelanja online dan kasir tidak bisa scan/gesek kartu Anda, tiga digit kode ini yang bisa membuktikan ini adalah kartu milik Anda.

Jika penipu sudah memiliki nomor kartu, tapi tidak memiliki kode ini, maka transaksi tidak akan berhasil.


OCBC