Security Awareness

A guide to credit card acceptance

WHAT YOU WILL LEARN

- ❑ Card Present Transactions
  - ❑ Know your terminal
  - ❑ Know your cardholder
  - ❑ How to recognize a counterfeit card
  - ❑ The difference between a valid card and a counterfeit card
  - ❑ Basic security tips
  - ❑ What to do about a suspicious card

- ❑ Telephone Transactions
  - ❑ Identify the customer
  - ❑ Card security codes

- ❑ Protecting the Company Network
  - ❑ The importance of Passwords
  - ❑ Acceptable use of the network and computers
  - ❑ Cautions about email attachments
  - ❑ Preventing unauthorized access
    - ❑ People
    - ❑ Things

- **Know your terminal and devices**
  - Terminals have recently become a source of fraud through tampering. Thieves commonly do this in several ways:
    - Switching terminals
      - Most commonly, individuals, working in pairs, take your terminal and replace it with one of theirs that takes YOUR transactions and settles them to THEIR bank account. They leave the terminal behind and may never come back. Usually they take the stolen terminal (yours) and reprogram it to steal from the next business they victimize.
      - Tampering is also a problem with both attended and unattended terminals, and ATM's. Thieves will often place a very small card reader inside the swipe slot or on an overlay that looks like part of the terminal. Their reader will either send the information or record it for them to retrieve later. Sometimes they put a camera in the vicinity to record PIN numbers
      - In another theft a few years ago the thieves came in a commercial van, wearing uniforms, and changed all the computerized cash registers at a major retailer. The cash registers worked normally but recorded the swipe data from the cards and sent it to the crooks, who used it to make counterfeit cards.
    - What can I do to stop this from happening to me?
      - Read on – next page.

- **Know your terminal and devices** - Continued

  - **What can I do to stop this from happening to me?**
    - **Know and protect your equipment**.

    - Have a guide with photographs, serial numbers, special marks, etc. that you can use to identify your equipment and readily see whether it is the same equipment as you had the last time you looked.
    - Inspect your equipment at least everyday. Inspect the area around the device to make sure there is nothing that doesn't belong there (like cameras). Keep in mind that these devices are meant to **not** be detected, they may be tiny!
    - If you do leave the area, inspect again when you return.
    - In small businesses and businesses with stand-alone terminals, place the terminal under lock and key when your business is closed.
    - Check the batch at the beginning of each day and make sure it is empty and that the batch number is consecutive from the day before. Some thieves will sneak in and run a batch of credits to their own cards, and worse.
    - Never let anyone touch or repair any equipment unless you know in advance they are coming and verify that they are who they say they are.

- **Know your terminal and devices** - Continued

  - What if I notice something wrong?

    - Don’t take any transactions through the device
    - Call your merchant services provider on the number printed on your statement
    - Lock up the device to prevent further tampering
    - Talk to the manager or owner for further instructions
    - Notify the person responsible for Incident Management

❑ Card Present Transactions

In person credit card fraud has been a problem since credit cards became popular decades ago. Remember that counterfeit cards are used by people who are experienced at this type of fraud and know how to manipulate the system and have all kinds of tricks up their sleeves. These people can be quite bold and "pushy" when trying to use a fake card. You must be on your guard. We are going to go over a few things to look for.

Counterfeit cards come in 3 basic forms

- Stolen cards
- Counterfeit blank cards with real account numbers on them
- Real cards that have counterfeit magnetic strips

We will look at these one at a time, but first a word about Security Codes.

Security codes are printed on all cards. On American Express cards the code is 4 digits printed on the front of the cards above and near the end of the card number. On the other brands it is the last 3 digits on the signature panel.
Printed on the card is the only place this number appears. If this number is written down or stored anywhere else, it compromises the security of that card and anyone else who accepts it. That is why it is important that the security code is never written down or stored in any way.
If prompted by your terminal or system, enter it. If it doesn't match…do not accept the transaction.

- **Know your cardholder**

A card that has been stolen looks like a any other card and, if it hasn't been reported stolen, the transaction might be authorized. The only thing wrong is that the person holding it is not the authorized card holder.

This is why you must routinely and politely verify that everyone who presents a card for any transaction is the authorized person.

Cards are not valid unless they are signed in ink (It says so on the signature panel).

Obtain an authorization, have the customer sign and compare the signature on the receipt to the signature on the card. If it doesn't look right it is appropriate to POLITELY ask the customer for identification. While the rules do not permit you to ask every customer for identification, if you are suspicious, you may ask.

If "SEE ID" is written on the signature panel. By rule these cards are not valid and you do not have to accept them. Remember – it is easier to forge a photo ID than a credit card. Some companies have a policy that they will accept these transactions in the interest of good customer relations, but understand that you are taking a risk that the cardholder is not who he or she says he is.

- **Know your cardholder** - continued

Transaction declines are an every day occurrence and it is here that you have to use all of your customer service skills.

Declines must always be handled POLITELY (we are going to use that word a lot) because they have a variety of causes, most of them are not criminal, and they are not always because of credit problems. The best approach to take is to politely tell the customer that the authorization was declined ask for another form of payment. If the customer is insistent, you may call for authorization at a number that you have received from your bank or provider, and seek an authorization code. Or you might suggest the customer call the number on the back of the card and see if he can clear it up. If the customer clears it up you should be able to obtain an electronic authorization immediately. NEVER, EVER accept an authorization code from an incoming call. Banks will not give you an authorization code from a customer phone, nor will they call you. The transaction is only secure if **you** initiate it!

If none of this works, the customer will have to provide another form of payment.

Forcing transactions – is when you press a key on the terminal or computer (usually labelled 'FORCE') and enter the authorization code you received from the operator who YOU called. It is important to realize that once you press that key, the transaction will be accepted by your terminal. If the authorization number is not valid and the card is not authorized, you will receive a chargeback and the money for the transaction will be taken away.

- **Card Present Transactions**
  - **Counterfeit blank cards with real account numbers on them**

This is not the most common form of fraud there is, but it happens, and it can happen to you. Here we will tell you about how to recognize a fake card and tell you where to look for a reference (the back of this document). Pull out the last 4 pages and follow along.

Legitimate credit cards are manufactured to precise standards under highly secure controls. They have built in security features that are hard to duplicate and even if some features are duplicated it is not very likely that they all are duplicated. Study the guide so you can spot a fake, then use the guide for comparison if you think you have a counterfeit.

Some things about genuine cards

Number, Expiration Date, and Cardholder name are embossed and the letters and numbers always line up across the card. Misaligned numbers indicate that someone has a cheap embossing machine in their basement. The embossing extends into the hologram.

They have holograms on the back that change when shifted in the light. They also have micro-printing and/or numbers printed on the signature panel (hard to fake). Many other features are on the guide(s) – get to know them.

Also, a black light comes in handy for cards as well as cash and ID's.

- **Telephone/Internet Transactions and any other transaction where the card is not present. This means that you do not have the card in your hands.**
  - **Identify the customer**
    - Apart from the normal questions you may ask your customers, when you get to the credit card information there is a useful service called AVS. Address Verification Service (AVS) matches certain elements of the cardholder information to information on file such as, Cardholder Name, the numbers in the address and the zip code. We recommend that you have your processor make AVS available to you and that you become familiar with, and use it. Some interesting facts about AVS.
      - Close to 100% of counterfeit cards receive a NO MATCH response for all elements of AVS.
      - 90% of cards stolen from the mail received a NO MATCH.
      - 65% of stolen cards, same thing.
      - AVS is done differently by different processors, so check with your provider to see how AVS applies to you.
  - Card security codes
    - Security Codes are three digit codes that appear on the signature block of most cards brands. On American Express it is a 4 digit code on the front of the card (see guide for more)
    - The only place the code appears in writing is on the card, so if the customer knows this number, it is a pretty good bet that the person you are talking to has the card.
    - Never accept a transaction if the security code is wrong.

- **Protecting the Company Network**
- **Everything presented here is based on the Acceptable Use, User Passwords and other policies. These policies describe the front line of network security…You, the user. Pay attention to these policies. Understand them. Follow them. There is an unending stream of cases where someone who was not authorized accessed a network by tricking someone into giving out a password or attaching a damaging device. Please don't be careless about computer access, it can cause great damage.**

  - Passwords are the key to the front door, whether at work or home. Once someone is in the front door of a computer network, security diminishes with each additional door opened. Sure the jewelry is in a safe (like encryption keys), but lots of other things are vulnerable. The longer the burglar is in your network "house," the more trouble he can make. Let's keep him out.

    - Use strong passwords of at least 8 characters using UPPER and lower case letters, some numbers and $peCi@L Ch@r@cters. Make them so they mean something to you, so you can remember them. If you like S3@_$@lt_p0t@to_cH1p$ (sea salt potato chips) - you can make them into P@ssw0rd$. These kinds of passwords are really hard to hack.
    - Change them often. At least as often as your company policies require.
    - No sharing. Unauthorized access aside, someone could use your name/identity and cause you harm.
    - Keep it secret. Don't write it down or leave it laying about.
    - Don't use another persons password.
    - Do follow the Password Policy and everything it says.

- **Protecting the Company Network** - Continued

  - This section gives some explanations of a few subjects covered by the acceptable use policy. The policy itself has more information, but these highlights should help you understand the importance of exercising caution when using company computers or, for that matter, your home computer.

    - The Internet is a risky place
      - On the order of 90% of attacks on networks came from the internet last year.
        - If a website tells you that you can't see the picture of the cute kitten playing because your version of Java is out of date…and "Click here to download the update." Don't, it is probably a trick. Never download or install software unless it is from a trusted source.
        - Download software only if you or a legitimate program on your computer initiates it.
  - **Cautions about email attachments and links**. Email attacks are usually about social engineering, that is, making someone think they can trust the sender and then launching an attack.
    - Emails even from people you know might not be trustworthy because they themselves may have been tricked into forwarding a malicious email. Don't necessarily trust someone else's ability to detect fraud.
    - Emails from people you think you know may not really be from people you know. Usually your virus and spam filter will identify these - delete them.
    - Emails from companies you know, like your bank, containing links. As convenient as it is to use the link, it is a common attack. Navigate to your bank on your own and logon to find out shat they want.
    - Emails with grammar and spelling problems. Everyone knows about the Ethiopian Prince scam, but the lesson is that if a message has language problems, delete it.

- **Protecting the Company Network -** Continued
  - Unauthorized parties take 2 basic approaches to gaining access. One uses people, the other uses things, sometimes in combination with people. Both use social engineering. There is a third way involving electronic and/or physical attacks which we will not address here.

    - People
      - A common way people are manipulated is by convincing them to reveal a password. In a recent incident an attacker convinced a support person that he was the CEO of the company and needed his password reset. The support agent violated procedure and sent the password to the attacker. Before discovery the attacker had erased (probably after copying) some of the CEO's correspondence. Other password compromises have allowed attackers to get access to email and find out confidential information.
      - As we have said before, sharing or telling another your password is dangerous and absolutely forbidden.

    - Things – Attacking by attaching devices is another way of planting malicious software in networks or intercepting data.
      - Recently some foreign made devices were discovered to come from the factory with malware pre-installed. Very few realized this and many computers were recruited for a bot-net.
      - A thumb drive dropped (planted) in a building with a label saying "Executive Compensation" displayed an error message and uploaded a virus. It was passed to several curious employees…
      - Devices hooked up to unused network jacks could be planted and monitoring network traffic. If you see something suspicious. Report it!

- **Links to Card Security Feature sites:**

  - American Express - https://secure.cmax.americanexpress.com/Internet/International/japa/SG_en/Merchant/PROSPECT/WorkingWithUs/AvoidingCardFraud/HowToCheckCardFaces/Files/Guide_to_checking_Card_Faces.pdf
  - Discover - http://www.discovernetwork.com/merchants/fraud-protection/prevention.html
  - MasterCard - http://www.mastercard.com/us/merchant/pdf/MST08004_CardFeatures_r4.pdf
  - Visa - http://usa.visa.com/download/merchants/card-security-features-mini-vcp-111512.pdf
  - JCB - http://www.discovernetwork.com/common/pdf/JCBCardIdentificationGuide.pdf

MasterCard® Card Security Features

Card-specific security features on MasterCard cards.

Every MasterCard card includes a variety of security features that are designed to effectively protect cardholders from payment card fraud. Security features on MasterCard cards include:

- **Magnetic stripe.** The film stripe on the back of a MasterCard card stores account information. The magnetic stripe does not contain personal information such as birth date or mother's maiden name.
- **Embossed numbers.** Raised account numbers on the front of a MasterCard card extend into the hologram (if a hologram is on the card face).
- **Tamper-evident signature panel.** The signature panel on the back of a MasterCard card guards against fraudulent use.
- **Personal Identification Number.** The cardholder's PIN protects ATM and debit transactions.
- **Card Validation Code 2.** The three-digit code indent printed on the signature panel of a MasterCard card enables retailers to ensure that the cardholder has possession of the card during a phone or online transaction.
- **Hologram.** A three-dimensional image with interlocking globes reflects light and appears to move when the card is rotated.
- **Holomag™.** This feature combines the functionality of the magnetic stripe with the security of a hologram and helps prevent card counterfeiting.

MasterCard. SecureCode.

Safer Shopping Online

MasterCard® SecureCode™ creates an extra level of authentication for your purchases at participating e-tailers preventing unauthorized use of your card.

Learn More

VISA CARD
SECURITY FEATURES

The **Signature Panel** must appear on the back of the card. The words "Authorized Signature" and "Not Valid Unless Signed" must appear near the signature panel. If tampered with, the word "VOID" will be displayed.

The **Mini-Dove Design Hologram** may appear on the back on either side of the signature panel or on the front of the card above the Visa brand mark.

Card Verification Value 2 (CVV2) is a three-digit code that appears either on or in a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel.

Account Number on valid cards begins with "4." All digits must be even, straight, and the same size.

Visa Brand Mark must appear in blue and gold on a white background in either the bottom right, top left, or top right corner.

Visa Chip cards are embedded with a chip. At this time, chip cards are primarily issued outside the U.S.

Expiration or "Good Thru" date should appear below the account number.

Four-Digit Bank Identification Number (BIN) must be printed directly below the account number and must match exactly with the first four digits of the account number.

© 2012 Visa Inc. All rights reserved. VPC 11.15.12

Discover® Network Card Identification Features

The words "DISCOVER NETWORK" will appear under an ultraviolet light.

All Discover Network account numbers start with 6. Embossed card numbers should be uniform in size and spacing, and extend into the hologram. Unembossed cards may display account number and expiration date printed flat on the front.

"Valid Thru" indicates the last month in which the card is valid.

A Business Name may be embossed below the account name.

Embossed Security Character appears as a stylized "D." No stylized "D" appears on unembossed cards.

Some cards may display a hologram on the card front with a globe pierced by an arrow. There is no hologram on the card front if the card back displays a holographic magnetic stripe.

The magnetic stripe should appear smooth, with no signs of tampering. Some cards display a holographic magnetic stripe with blue circles.

The words "DISCOVER NETWORK" appear on a tamper-evident signature panel.

The last four digits of the card number are displayed on the signature panel in reverse indent printing.

The three-digit CID is printed in a separate box to the right of the signature panel on the card back.

The Discover® Network Acceptance Mark will appear on the front and/or back of the card.

Law Enforcement Phone Line
1-800-347-3083
for law enforcement officers

Merchant Code 10 Authorization
1-800-347-1111
for suspicious transactions

American Express® Card Identification Features

The letters "AMEX" and a phosphorescence in the Centurion portrait are visible under an ultraviolet light.

Preprinted (non-embossed) Card Identification Number (CID) should always appear above the account number.

Do not accept a card after the expiration date.

Only the person whose name is embossed on an American Express Card is entitled to use it.

All American Express account numbers start with 3. Embossing should be clear and uniform in size and spacing. The number on the front and back of the card, plus the one printed on the sales receipt should all match.

With this statement on the card, American Express reserves the right to "pick up" the card at any time.

Some cards have a hologram of the American Express image embedded into the magnetic stripe.

The signature on the back of the card should match the customer's signature on the receipt. The signature panel is tamper-evident.

Merchant Code 10 Authorization

1-800-528-2121

If you are suspicious of a card transaction