paynamics

The **Evolution** of Online Payment Services

Online Credit Card Payments

Digital Filipino E-Commerce Bootcamp (March 9, 2015)

paynamics

Outline

A. Credit Card Payment Transaction

- Parties Involve in a Credit Card Payment Process
- Credit Card Process Flow

B. Getting a Credit Card Merchant Account

- Qualifications
- Application Process
- Service Charges and Conditions

C. Fraud, Risk and Chargeback Handling

- Understanding the Risk
- Potential Fraud Signs
- Why Fraud Matters
- Best Practice in Preventing Fraud
- Difference between Fraud and Chargeback
- Best Practices for Chargeback Handling

Credit Card Payment Transaction

Parties

Customer

- This is the person who has the intention to make an online purchase.
- This person may or may not own the credit card being used for the intended online purchase.

Online Merchant / Seller

- This is a business entity that sells and fulfills the goods and services.
- This business entity also handles cancellation, disputes and refunds requests coming from the customer.

Parties

Issuer

- This is the business entity that issues the credit/ card to the customer.
- This entity is a member of the card network.
- Banks are the biggest issuers of debit/credit card in the Philippines (i.e. HSBC, Citibank, etc)

Acquirer

- This is the business entity that provides the credit card merchant account in order to process and clear an online transaction.
- This business entity clears and settles the merchant for successful payment authorizations.
- Sample Philippine Banks that provides an online merchant account are BDO, BPI and Maybank.

Parties

Card Scheme / Card Network

- This is the entity that is responsible for routing payment authorization and settlements in between the issuers and acquirers.
- This entity also establishes the rules and regulations governing card present and card not present transactions.

Payment Service Provider

- This entity is responsible for providing the technical connectivity between the merchant and acquirer.
- This entity provides merchant an easy to use and secure payment integration package that allows merchant to create positive payment experience.
- This entity may provide fraud detection and mitigation, that protects merchant from processing fraudulent transactions.

Credit Card Process Flow

1 Customer goes to merchant website to shop.
2 Customer checks out and proceeds to Paynamics Payment Page.
3 Once customer press submit, Payment page connects to Paynamics Gateway Application Host (Paygate). Paygate performs fraud detection and mitigation of the given transaction.
4 If transaction is good, Paygate connects Acquirer Host for payment authorization.
5 Acquirer connects to Card Network.
6. Card Netwrok connects to Customer's Issuer for Authorization Approval.
7 Issuer sends approval/authorization response to Card Network.
8 Card Network relays response to Acquirer.
9 Acquirer relays response to Paygate.
10 Paygate relays response to Payment Page.
11 Payment Page shows Transaction Status and will send URL notification to merchant shopping cart system. This is in order for merchant shopping cart to tag the transaction as successful.
12. Merchant Shopping Cart updates order to success and notifies the customer that the order will be processed

Getting a Credit Card Merchant Account

paynamics

Qualification for a Credit Card Merchant Account

Minimum Requirements

- Startup or Established Business in Good Standing (i.e. Single Proprietorship, Partnership, and Corporation).
- Website (For Retail or Digital Goods).
- Bank Account with the Acquirer.
- Physical Office.
- Compliant Products and Service. (Not in acquirer's negative products and services)
- Policies and Procedures (Refund, Cancellation and Dispute).

Conditional Requirements

- Order Process Flow and KYC Process
- Special Licenses (i.e. IATA License for Travel Agents)
- Security Bond (ranging from 100K to 1Mk depending on merchant category).
- Fraud Tool Provider.

Application Process

Step 1
Pre-Application

1. Submission of Pre-Application Form
2. Submission of Business model summary.

**Note: At this stage, Paynamics Account manager will contact Payment Acquirers (i.e. BDO, BPI, and Maybank) for merchant pre-approval.

3. Merchant Acceptance Sign Off.

Step 2
Full Application

1. Collection of Merchant Documents. (Please refer to Merchant Compendium) and other Business compliance docs (i.e. Website Compliance Checklist, etc.)
2. Signing of Documents by Appropriate Parties
5. Bookkeeping of KYC Documents and further submission of KYC docs to Payment Acquirers.
6. Payment of Setup Fees.
7. Merchant Account Manager Signoff

Step 3
Technical Integration

1. Release of Application Programming Interface
2. Creation of Test Accounts and Merchant ID.
3. Technical Manager User Acceptance Test Sign off

Step 4
Training Session

1. Risk Management Training with Key operations personnel and beneficial owner.
2. Merchant Back Office Training with Accountant and beneficial owner
3. Trainer Signoff

Step 5
Live

1. Acquirer will provision production credentials to Paynamics Technical Team.
2. Paynamics Technical will issue Live Merchant Credentials to merchant.

Service Fees and Conditions

Acquirer Fee and Conditions (Credit Card)

- **Setup Fee:** $400.00 USD
- **Merchant Discount Rate:** Between 2.5%-5.5% (Rates will heavily depend on Risk, Merchant Business Model, Volume and Merchant Standing).
- **Average Ticket Amount:** Some acquiring bank may require an average ticket amount of Php 2,000 and above
- **Minimum Monthly Volume**: Some acquirer may require a minimum monthly volume of Php 120,000 or more.

Payment service provider Fees and Conditions

- **Setup Fee:** Between Php 15,000 – 55,000 (Dependent on merchant risk model, customization options, payment methods enabled and Merchant Life Time Value.)
- **Merchant Discount Rate:** 0.4%-1.0% (Dependent on merchant risk model, customization options, Payment Volume and Merchant Life Time Value.)
- **Transaction/Gateway Fee:** Php 6.00 – 12.00 (Dependent on merchant risk model, customization options, Payment Volume and Merchant Life Time Value.)
- **Monthly Fee or Renewal Fee:** May Vary depending of service provider.

Fraud, Risk and Chargeback Handling

paynamics

Understanding the Risk

- **Burden of Legitimacy**- For Card-not-present (Online or Mobile) the burden of proving the transaction is "legitimate" is with the merchant. (This is contrary to P.O.S. swipe transaction in which the burden of legitimacy is with the cardholder).

- **Place of Transaction** – Card-not-present happens online, having the customer transacting at their own convenience without going to the merchant premises. There is a risk that the person transacting may not be the same person as what he claims to be.

- **Credit Card Black Market** – mIRC chat, carder forums are "havens" for "schemed" or stolen credit cards. Credit card information can be bought in these markets.

- **Dispute Rights** – Cardholders have the right to dispute up to 180 days from the date of fulfillment of the transactions. For merchants, an approved and settled card transaction does not exempt from this potential liability.

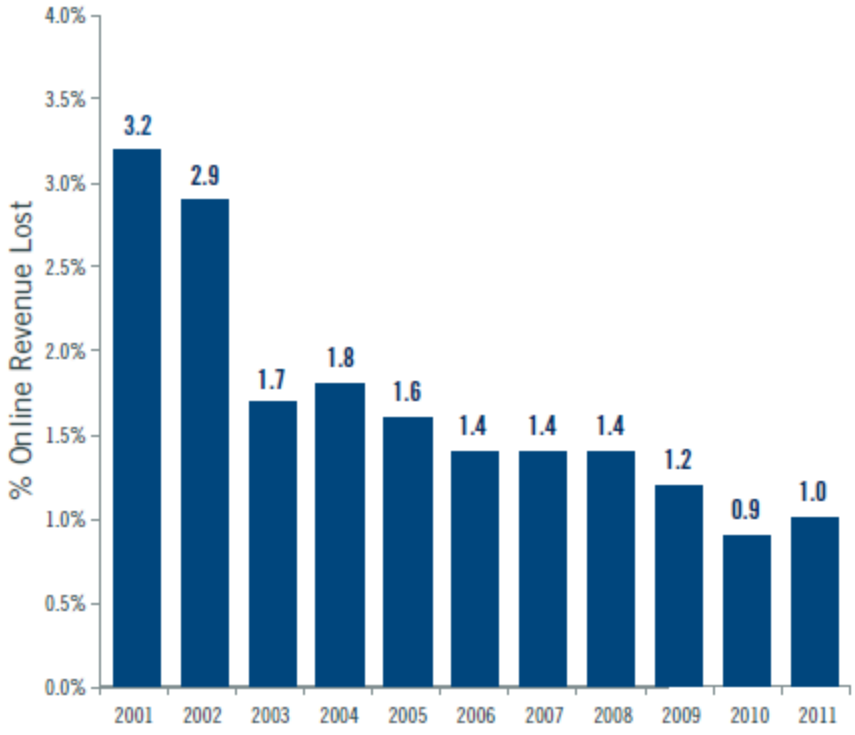
Understanding the Risk

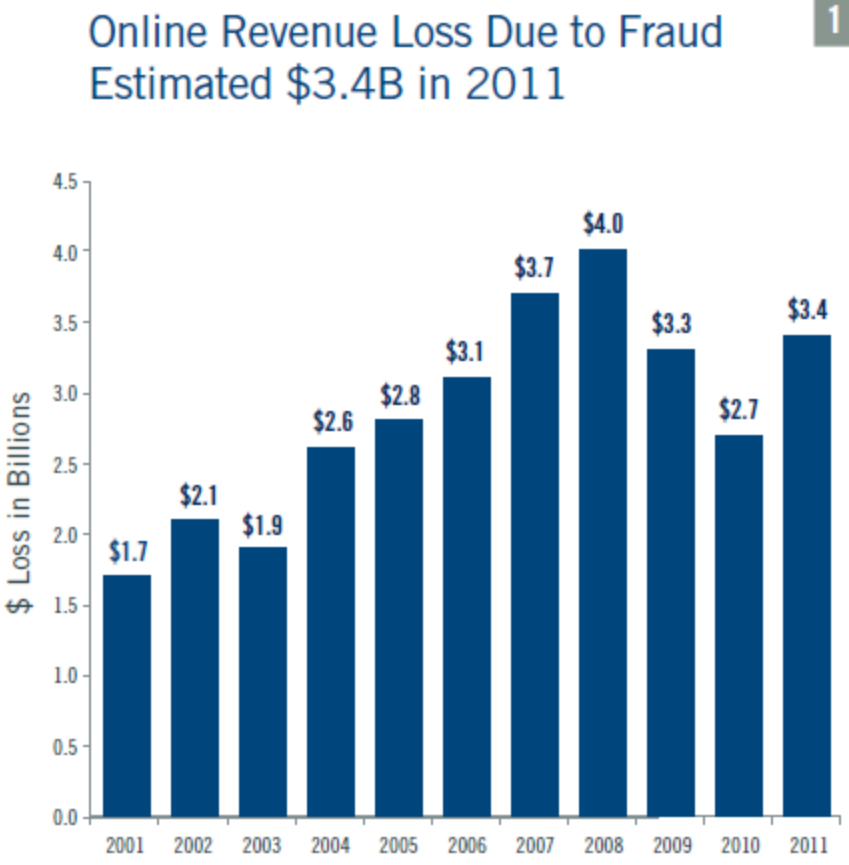
Cybersource 2013 Report

- Ecommerce (Card not present) sales are rising 12% year on year.
- Merchant online fraud losses continued to increase, reaching a peak of $3.5 billion in 2013.
- In 2012, merchants estimated they lost 0.9% of online revenues to fraud
- In 2012, fraud risk on international orders averaged 1.6%.
- Average ticket size of a fraudulent order is $200 USD. Average ticket size of a valid order is $149 USD

paynamics

Understanding the Risk





paynamics

Potential Fraud Signs

1. First-time shopper: Criminals are always looking for new victims.

2. Larger-than-normal orders: Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchase.

3. Orders that include several of the same item: Having multiples of the same item increases a criminal's profits.

4. Orders made up of “big-ticket” items: These items have maximum resale value and therefore maximum profit potential.

5. “Rush” or “overnight” shipping: Crooks want these fraudulently obtained items as soon as possible for the quickest possible resale, and aren’t concerned about extra delivery charges.

paynamics

Potential Fraud Signs

6. Shipping to another address: A significant number of fraudulent transactions are shipped to countries outside the country of transaction origination.

7. Transactions with similar account numbers: Particularly useful if the account numbers used have been generated using software available on the Internet.

8. Shipping to a single address, but transactions placed on multiple cards: Could involve an account number generated using special software, or even a batch of stolen cards.

9. Multiple transactions on one card over a very short period of time: Could be an attempt to "run a card" until the account is closed.

paynamics

Potential Fraud Signs

10. Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses: Could represent organized activity, rather than one individual at work.

11. In online transactions, multiple cards used from a single IP (Internet Protocol) address: More than one or two cards could indicate a fraud scheme.

12. Orders from Internet addresses that make use of free e-mail services: These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

paynamics

Why Fraud Matters?

- **Merchant Liability:** Merchants are liable for Fraud. Card Networks or Acquirer may penalize the merchant exceeding fraud thresholds.

- **Brand Damage Reputation:** Merchants that have high fraud ratios are at risk of brand damage from customers and other stakeholers.

- **Termination and Blacklist Risk:** Merchants that are terminated due to fraud are also blacklisted by the Card Network. This may effect future merchant account applications by the merchant with other acquirers.

paynamics

Best Practice in Preventing Fraud

1. **Determine early on the qualities and behavior of your Good Customer vs your Bad Customers–** Before launching your business, research on other business that is similar to yours and pre-determine the behavior of your good customer. By establishing this early, will give you a headstart in understanding your business especially once fraud occurs.

2. **Look into your business transaction** - To some extent, the more time you spend on investigate into your transactions, the lesser chance you are swindled by fraud. Check into the I.P. address billing and shipping address of your clients. Can help you determine if the client is a normal customer or a potentially fraudulent customer.

3. **Transaction Flow** – Always verify Customer (though Email feedback, Call Feedback) It is highly recommended to build membership on your e-tailing or e-commerce web site.

paynamics

Best Practice in Preventing Fraud

4. **Formulate your own Risk Policy** – It is always important to have a company procedure to handle online transactions. The risk policy should adopt to your business model.

5. **Partner with the Right Service Provider –** As ecommerce grows, fraud also grows. Merchants nowadays can fight fraud by partnering with the right payment service provider that can help them determine fraudulent transactions and prevent it from transacting in their business. Qualities of a great service provider are the following:
   - ❑ **Extensive experience in fraud detection and mitigation.**
   - ❑ **Can provide automated and scalable fraud detection tools that is easy to understand and interpret.**
   - ❑ **Can provide custom fraud policies that can mitigate fraudulent transaction from entering your business.**
   - ❑ **Can provide training and analysis to your operations team to increase fraud awareness.**

Difference of Fraud and Chargeback

Definition of Chargeback: Chargeback is a refund requested by the cardholder to his/her Issuer then eventually it is being forwarded to the Acquirer and Merchant for further processing.

Causes of Chargeback:

1. **Fraud related chargeback** – These are customers claiming that they did not authorize the transaction. Some cases involves card transactions that are ultimately are reported as "schemed" or "stolen" by the issuers.
2. **Merchant related chargeback** – These are chargeback caused by the merchant. Samples are:
   - Merchant did not deliver the product/service or the product and service delivered was not as described.
   - Merchant did not deliver the product/service on time.
   - Merchant process the transaction twice (duplicate transaction)

paynamics

Best Practice for Chargeback Handling

1. Act promptly in issuing refund/credits to customers with valid dispute. Customers that are displeased may escalate this to a chargeback with their issuer.
2. Let cardholders know immediately of the impending credit.
3. Respond to a customer complaints as quickly as possible.
4. Address all of the cardholder's pertinent claims. If the complain is resolved, it is good to obtain a written or email consent that the dispute was already resolved, and you as the merchant are cleared of any issues related to the complaint.
5. In times were the cardholder is denying the existence of the payment transaction, be sure to supply "compelling" information to prove the true cardholder participated in the transaction, received the goods or services, and benefited from the transaction.

Thank you for sharing the vision.

Ronald Gerald P. Magleo

Founder and CEO

Paynamics Technologies Inc.
Suite 1108 Cityland 10 Tower 2
H.V. Dela Costa St., Salcedo Village
Makati City 1227 Philippines

eMail: ronald.magleo@paynamics.net
Website: http://www.paynamics.com