Consumer Identity Authentication and Verification

Janette Toral

DigitalFilipino.com

Order Screening Process

What to Look For In an Order?

Meta Data	Description	Risk Signs	Tools for Checking
Name	Billing Name, Shipping Name, Cardholder Name	• If all info are the same the lower the risk. • For travel merchants, different cardholder name from billing name is a norm. • For retail, different carholder, billing and shipping is considered high risk.	• Google Search • Linked In • Facebook • Previous Customer Data
Contact Info (Email)	Email	• Free email is riskier than domain email. • If email username is the same as Name, the lesser the risk. • Fake Email Domain Generator are an automatic redflag	• Check email domain at whois.net • Check fake email generators
Device I.P. Address	I.P. Address of customer	• An Order is riskier if Device I.P. country is different from Billing Country or Shipping Country	• Ip2location.net
Contact Info (Phone)	Phone number or Mobile Number	• International Phone numbers are riskier that local phone numbers. • Non contactable phones are risker.	

Source: Ronald Magleo, Paynamics

What to Look For In an Order?

Meta Data	Description	Risk Signs	Tools for Checking
Payer Authentication Level	3D Secure vs Non 3D Secure	- Non-3D secure transactions are riskier.	- Payment Provider Dependent
Address	Billing and Shipping Address	- Different Shipping and Billing Address are riskier. - Address that shows a gasoline station, inn or hotel is considered high risk.	- Google Maps
BIN	Bank Identification Number	- Foreign Issuers are considered riskier than domestic issuers. - Credit cards are more riskier than debit cards in is some countries. - Issuing Banks that are reported in a Data Breach are considered High risk	- Payment Provider Dependent
Device ID	Device Signature that has access your account	- Transactions that have the same Device Signature are riskier	Payment or Fraud Provider Dependent

Source: Ronald Magleo, 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.

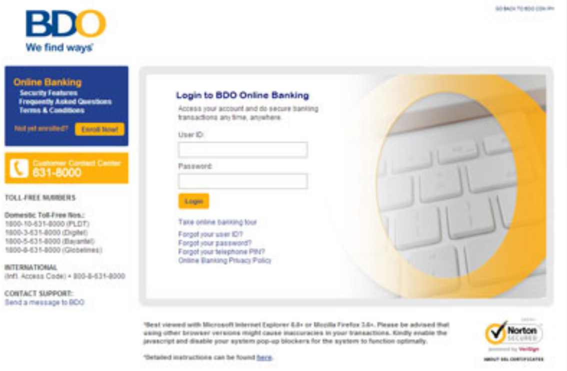
- **Credit Card Black Market** – mIRC chat, carder forums are “havens” for “schemed” or stolen credit cards. Credit card information can be bought in these markets.

- **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.

Source: Ronald Magleo, Paynamics

Fraud #1:
Online Banking Identity Theft

- Difficult to perpetrate because:
  - Complex id/pwd system
  - Can be changed anytime
- Online banking transactions are difficult (if not impossible) to repudiate



TOLL-FREE NUMBERS

Domestic Toll-Free Nos.:
1800-10-631-8000 (PLDT)
1800-3-631-8000 (Digitel)
1800-5-631-8000 (Bayantel)
1800-8-631-8000 (Globelines)

INTERNATIONAL
(Int'l. Access Code) + 800-8-631-8000

CONTACT SUPPORT:
Send a message to BDO

Login to BDO Online Banking

Access your account and do secure banking transactions any time, anywhere.

User ID:

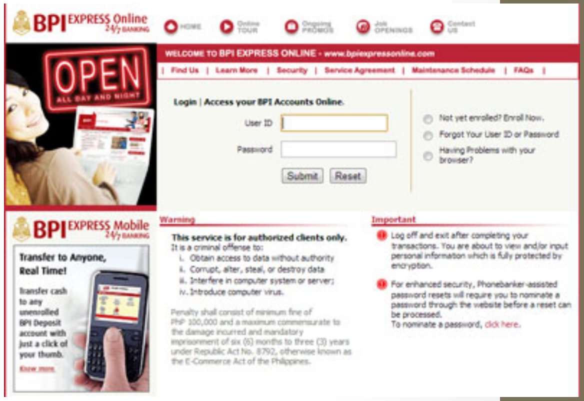
Password:

Take online banking tour
Forgot your user ID?
Forgot your password?
Forgot your telephone PIN?
Online Banking Privacy Policy

*Best viewed with Microsoft Internet Explorer 6.0+ or Mozilla Firefox 3.0+. Please be advised that using other browser versions might cause inaccuracies in your transactions. Kindly enable the javascript and disable your system pop-up blockers for the system to function optimally.

*Detailed instructions can be found here.

Norton SECURED
powered by VeriSign
ABOUT SSL CERTIFICATES


BPI EXPRESS Online 24/7 BANKING
HOME
Online TOUR
Ongoing PROMOS
Job OPENINGS
Contact US
OPEN
ALL DAY AND NIGHT
| Find Us | Learn More | Security | Service Agreement | Maintenance Schedule | FAQs |
Submit
Reset
BPI EXPRESS Mobile 24/7 BANKING
Know more

WELCOME TO BPI EXPRESS ONLINE - www.bpiexpressonline.com

Login | Access your BPI Accounts Online.

User ID

Password

○ Not yet enrolled? Enroll Now.
○ Forgot Your User ID or Password
○ Having Problems with your browser?

Transfer to Anyone, Real Time!

Transfer cash to any unenrolled BPI Deposit account with just a click of your thumb.

Warning

This service is for authorized clients only.
It is a criminal offense to:
i. Obtain access to data without authority
ii. Corrupt, alter, steal, or destroy data
iii. Interfere in computer system or server;
iv. Introduce computer virus.

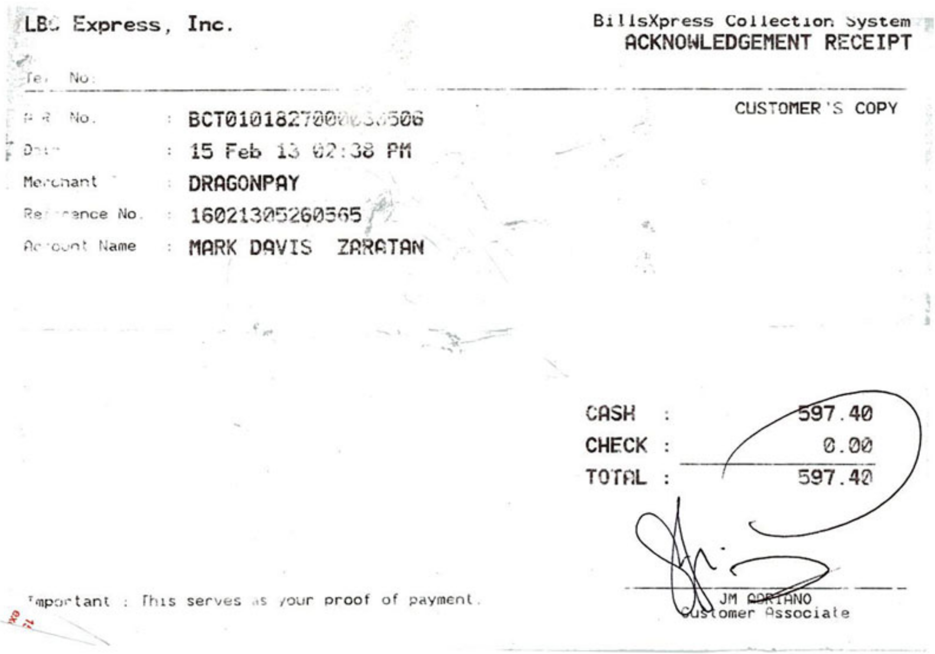
Penalty shall consist of minimum fine of PhP 100,000 and a maximum commensurate to the damage incurred and mandatory imprisonment of six (6) months to three (3) years under Republic Act No. 8792, otherwise known as the E-Commerce Act of the Philippines.

Important

- Log off and exit after completing your transactions. You are about to view and/or input personal information which is fully protected by encryption.
- For enhanced security, Phonebanker-assisted password resets will require you to nominate a password through the website before a reset can be processed.
To nominate a password, click here.

Source: Robertson Chiang, Dragonpay

Fraud #2:
Image Manipulation Fraud



LBC Express, Inc.

BillsXpress Collection System
ACKNOWLEDGEMENT RECEIPT

Tel. No:

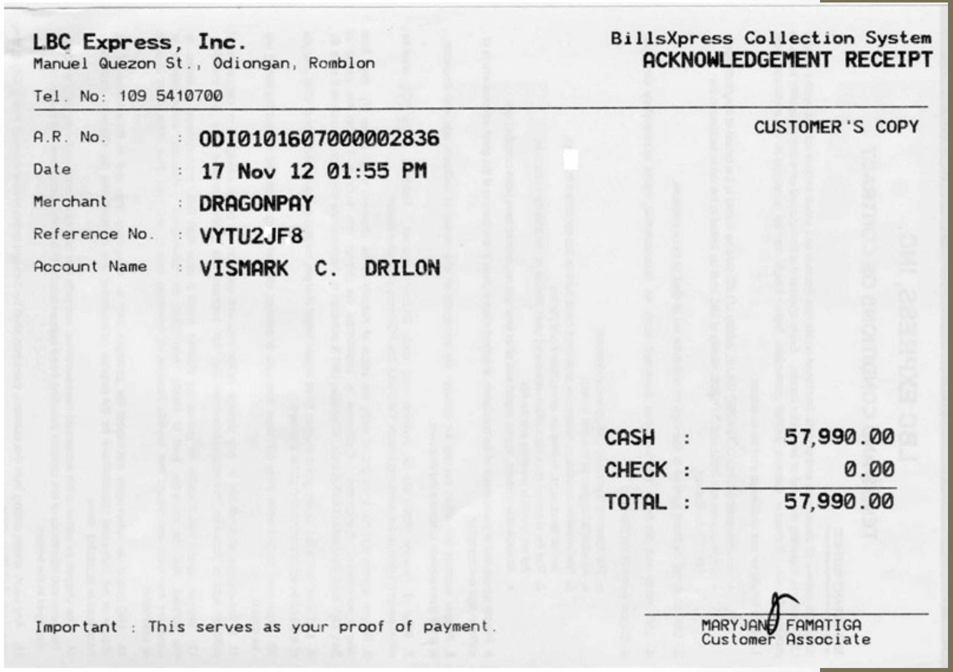
CUSTOMER'S COPY

A.R. No.	:	BCT0101827000030506
Date	:	15 Feb 13 02:38 PM
Merchant	:	DRAGONPAY
Reference No.	:	16021305260565
Account Name	:	MARK DAVIS ZARATAN

CASH	:	597.40
CHECK	:	0.00
TOTAL	:	597.40

Important : This serves as your proof of payment.

JM AARIANO
Customer Associate



LBC Express, Inc.
Manuel Quezon St., Odiongan, Romblon

BillsXpress Collection System
ACKNOWLEDGEMENT RECEIPT

Tel. No: 109 5410700

CUSTOMER'S COPY

A.R. No.	:	ODI0101607000002836
Date	:	17 Nov 12 01:55 PM
Merchant	:	DRAGONPAY
Reference No.	:	VYTU2JF8
Account Name	:	VISMARK C. DRILON

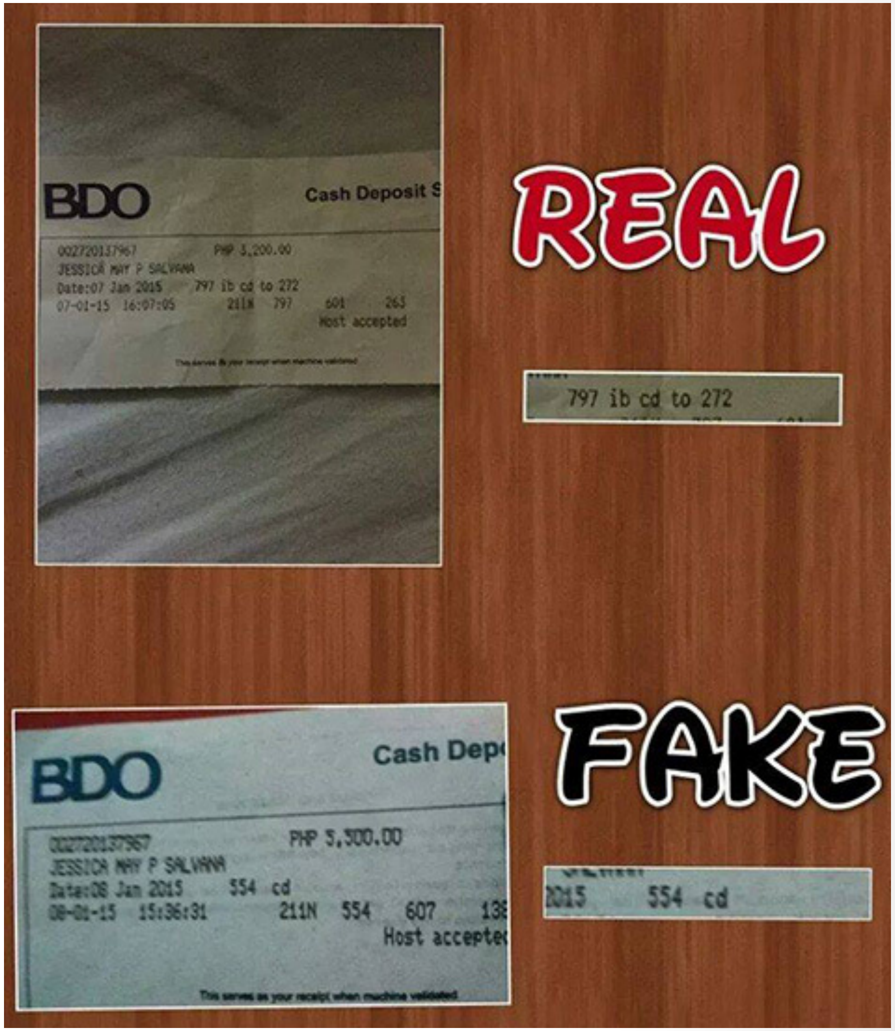
CASH	:	57,990.00
CHECK	:	0.00
TOTAL	:	57,990.00

Important : This serves as your proof of payment.

MARYJANE FAMATIGA
Customer Associate

Source: Robertson Chiang, Dragonpay

Fraud #3:
Fake Deposit Slip Fraud



BDO Cash Deposit S

002720137967 PHP 3,200.00
JESSICA MAY P SALVANA
Date:07 Jan 2015 797 ib cd to 272
07-01-15 16:07:05 211N 797 601 263
Host accepted

This serves as your receipt when machine validated

BDO Cash Dep

002720137967 PHP 5,300.00
JESSICA MAY P SALVANA
Date:08 Jan 2015 554 cd
08-01-15 15:36:31 211N 554 607 13
Host accepte

This serves as your receipt when machine validated

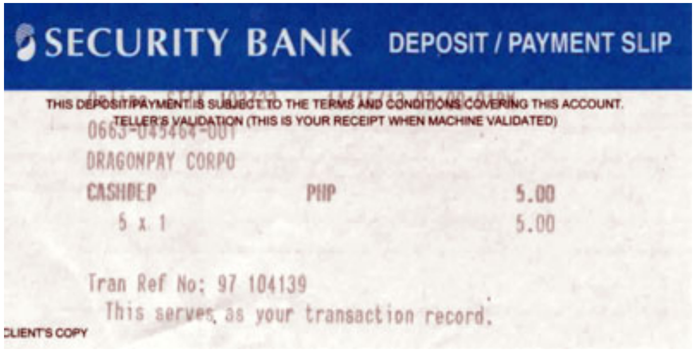
Source: Robertson Chiang, Dragonpay

Fraud #4:
Fake Mobile Notification Fraud

You have received 2,950.00 GCASH from Juan dela Cruz 09178561234. Your new balance is 7,950.00.
Ref. No. 294087757.

Source: Robertson Chiang, Dragonpay

Fraud #5:
Multiple Transmission of Payment



SECURITY BANK DEPOSIT / PAYMENT SLIP

THIS DEPOSIT/PAYMENT IS SUBJECT TO THE TERMS AND CONDITIONS COVERING THIS ACCOUNT.
TELLER'S VALIDATION (THIS IS YOUR RECEIPT WHEN MACHINE VALIDATED)

0663-045464-001
DRAGONPAY CORPO
CASHDEP PHP 5.00
5 x 1 5.00

Tran Ref No: 97 104139
This serves as your transaction record.

CLIENT'S COPY

Source: Robertson Chiang, Dragonpay

Fraud Prevention Tips

- Do not trust what “proofs” customer send you. Always check with the source (ex. Bank account, mobile wallet)
- If possible wait next day before checking the source.

Source: Robertson Chiang, Dragonpay

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.

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.

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.

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.

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.

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)

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.

E-COMMERCE ADVOCATE

Twitter:
@digitalfilipino
0917-4490011
Facebook: janettectoral

S3/1-12

BusinessWorld
weekender

EDITOR ALICIA A. HERRERA

I said, 'No one wants to see her boxing especially n you're roaching years old.'" Sylvester llone on his n Grudge atch

By Jasmine T. Cruz Reporter

Janette Toral is considered the "mother" of e-commerce in the Philippines, earning the title for her role in lobbying for an e-commerce law in the Philippines. The result was The Philippines E-Commerce Law - Republic Act No. 8792, which was signed in 2000 by then President Joseph Ejercito Estrada.

Mother, S3/2

Janette Toral has made a living online and teaches others how to do it

Mother of e-commerce

DIGITAL Leaders BOOTCAMP
#DIGITALLEADERS