How to Identify Credit Card Fraud?

In this tutorial, we would like to share with merchants some common techniques to pinpoint red flags of credit card frauds. Our goal is to cut down all frauds and chargebacks.

John is an online merchant selling watches. Below is one of his typical order. Everything looks fine to him but we would like to highlight some important information to help him make an informed decision.

Order Details		Billing Details		Shipping Details	
format	xml	payment_mode	CREDITCARD	ship_addr	12345 Boston Post Rd
ip (mandatory)	202.154.33.10	bill_city	New York City	ship_city	East Lyme
user_order_id	60625	bill_zip_code	10118	ship_zip_code	06333
user_order_memo		bill_state	New York	ship_state	Connecticut
amount	5400.00	bill_country	US	ship_country	US
quantity	3	bin_no	431940		
currency	USD	bin_bank_name	Bank of America		
department	ECommerce	bin_bank_country	US		
email_domain	mailinator.com	bin_bank_phone	6046102381		
phone	6046102380	card_hash*	4319400000000000		
email_hash*	fraud@mailinator.com	avs	Y		
username_hash*	acmin	cw	Y		
password_hash*	acmin				

IP Address

The IP address is from an anonymous web proxy service. It allows the user to hide their actual IP address but still perform an order submission. In this case, the actual user IP address is unknown and we only know the proxy server's IP address.

If we analyse the user's IP address, it is located in a different country which is 1,000 miles away.

Amount and Quantity

The order and quantity are also above average transaction values. Fraudster will usually order large quantities of items to maximize their returns.

Addresses

The shipping address is being listed as one of the forwarding service providers. The actual item will be forwarded to another address for collection upon fraudster's further instructions.

The shipping address, billing address and IP address locations are all totally different. In this case, the fraudster is using a proxy server, mail forwarder and stolen credit card to avoid tracking.

Email Domain

The order is being submitted using a disposable email address. The email address is easy to setup, anonymous and temporary.

Username and Password

The user name and password is too simple and generic. Fraudsters usually apply easy-to-remember account information.

Credit Card

The credit card number has been blacklisted due to prior exposure in public area. The fraudster purchased this credit card information from underground trading forums.

BIN and Issuing Bank

The BIN number and issuing bank name do not match. Fraudsters usually only have partial credit card information except the issuing bank information.

There are many other techniques that are not readily apparent when looking at the order forms such as transaction velocity and device fingerprints, both of which can also unmask a serial fraudster.

If you do not have the time to process these techniques for all orders, you can consider the FraudLabs Pro fraud service which is free for small businesses.

FraudLabs Pro service screens credit card transactions for online frauds. It accepts online transactions data via its open API. Fraud screening engine analyzes transactions parameters and returns its fraud analysis. Merchants can then decide on the next course of action based on the fraud distribution score or custom rules by conditions. Below are some features of FraudLabs Pro.

- Fraud analysis and scoring
- IP address geolocation & proxy validation
- Email address validation
- Credit card issuing bank validation
- Transaction velocity validation
- Device transaction validation
- Blacklist validation
- High risk username & password validation
- Export controlled country validation
- Malware exploit validation
- Custom rules trigger
- FraudLabs Pro Merchant Network
- FraudLabs Pro Merchant Administrative Interface
- Email notification of fraud orders
- Mobile app notification of fraud orders