everyoneapi

Fraud Mitigation and Identity Verification for Card Not Present Transactions

Overview

Credit card fraud costs businesses over $11 Billion dollars annually. The percentage of revenue lost to fraud is rising; increasing from 0.51% in 2013 to 0.68% in 2014. Losses to merchants are primarily from card-not- present (CNP) transactions from the Web, over the phone, or from mail order. In 2012 42% of Americans had experienced some form of credit card fraud in the last 5 years. [1] However, EveryoneAPI makes it possible to prevent fraud in even the most high-risk environments.

The challenge authenticating a customer in a card-not-present transaction is proving that the person making the purchase is the actual card holder. While this may sound trivial, it is nearly impossible to properly authenticate cardholders using the tools that traditionally have been available to merchants. Traditional address verification tools only verify that the supplied address matches the cardholder's billing address; it does not prove that the person placing the order has any association with the address they are supplying. For this reason, it is common for fraudsters to use stolen credit card information, as well as the card holder's real name and address, to make purchases. EveryoneAPI changes this by affording merchants the data they need to verify that the person placing the order is actually associated with the billing address they are supplying. This allows for real cardholder verification that is nearly impossible for fraudsters to defeat.

This paper will outline some of the current problems with identity verification for fraud mitigation, and present a solution that has reduced fraud by orders of magnitude in real world environments. Merchants can reduce fraud rates in high risk CNP transactions by verifying that the person making the purchase has possession of or access to a phone linked to the address on the credit card. Customers in risky transactions can be asked to enter a phone number, and quality data sources in conjunction with AVS can tie the phone number to the customer's billing address.

This solution and variations on it can help with multiple scenarios:

- Preventing fraudsters from using stolen credit cards
- Helping those Merchants who want to reduce fraudulent transactions
- Enabling credit card processing for merchants who are normally denied due to high risk of fraud. (These merchants are honest but are at high risk for fraudulent transactions due to their product or customer base.)
- Minimizing chargeback fees paid by merchants and improving their chargeback ratios.
- Reducing processing fees over time by presenting the processor with a low risk merchant account

- Minimizing Chargeback Fraud - By people lying about purchases they actually made. (It is harder to claim your transaction is fraudulent if you verified yourself.)

Standard Verification Tools Are Not Enough

AVS - Address Verification Service

Web sites today typically ask for the billing address of the credit card you use for payment. AVS or Address Verification Service then matches the entered address to the address associated with your card. If your credit card information has been stolen, on its own AVS simply verifies that the fraudster has access to your stolen information, which typically includes your address. AVS does not verify that the person making the purchase is the actual cardholder, thus leaving the merchant vulnerable to fraud.

However, additional information, that can be obtained using EveryoneAPI, can be used by the merchant to verify that the person placing the order is associated with the cardholder's address. By doing so, AVS becomes a tool that is safe for the merchant to rely on.

IP Address Geolocation

IP Address Geolocation has been touted as a solid solution to assist merchants in verifying orders. However, services are readily available that allow fraudster to place orders from the IP address of their choosing, and mobile IP addresses are rarely usable to obtain an accurate location. Legitimate travelers will also appear to be placing orders from the "wrong" location, resulting in lost sales for merchants. Even diligent merchants who attempt to check for VPNs or proxies can be defeated using malware on the cardholder's computer, which will cause the fraudster's IP address to match the cardholder's real address exactly. All of these problems can be remedied by using data from EveryoneAPI to properly authenticate the cardholder.

VPN Services

While VPN services can be legitimately used to protect privacy, it

is extremely common for fraudsters to use these services to fool IP Geolocation systems. Many VPN services are tailor made for the purpose allowing the user to appear from nearly anywhere in the world. If a fraudster wishes to use a stolen card from another country, or from a different part of his country, he may do so in just a few clicks.

There are services that purport to detect VPNs, but there are many drawbacks to using this approach. Customers who are legitimately using VPNs for privacy purposes will be blocked from placing orders. Due to the inaccuracy of these detection services, many VPNs will go entirely undetected, causing a false sense of security when a VPN is not properly detected.

Travel

Merchants who choose to use IP Geolocation as a primary factor will suffer severe conversion losses from travelers. If a customer is on the road, staying at hotel, or on vacation, they will appear to be placing orders from the wrong location. Determining the location of their IP address would only determine that a card holder making a purchase is not at home. It would not help determine the identity of the purchaser.

Mobile

Mobile traffic now exceeds desktop traffic. IP geolocation on mobile is incredibly inaccurate. Carriers often bundle traffic and push it to the internet at centralized locations, nowhere near the location of the actual mobile device. Tests in the field have shown that the difference between the location of the phone's IP address and the device's physical location can exceed 2,000 miles. Merchants who rely on IP geolocation will inevitably suffer conversion losses from mobile customers and potentially alienate a rapidly growing consumer segment.

Malware

It is becoming increasingly common for fraudsters to use malware to defeat IP geolocation. In these instances, the fraudster's IP geolocation

IP Address Geolocation

matches perfectly with the cardholder's billing address. Due to the fact that the order is not being placed through a commercial VPN or proxy service, but from the card holder's PC, there is no way for the merchant to detect this by looking at the IP address.

The fraud vectors described here can all be mitigated by authenticating cardholders using data from EveryoneAPI.

Verified by Visa and Mastercard Securecode or 3D Secure

3D Secure is the umbrella term for both of the Visa and Mastercard solutions that work by having the customer create a card-specific password.

When a customer places an order at a participating merchant, the customer is sent to another web site hosted on behalf of the issuing bank. If the customer's card is not already enrolled in 3D Secure, the customer is prompted to enter information, including social security number. The information requested during enrollment in to 3D Secure is readily available on the black market, including the social security number.

Potential for Fraud

There are several obvious problems with this scenario. Due to the fact that information required for enrollment is readily available on the black market, it is trivial for fraudsters to enrol the customer's card. On the other hand, if the customer's card is already enrolled, a simple keylogger can give fraudsters access to the cardholder's password. In many cases, keyloggers are not even necessary, as cardholders often use the same passwords across several accounts. These passwords are often sold on the black market, usually as part of a package that includes a great deal of the cardholder's sensitive information.

Consumers hate 3D Secure

Studies show that 3D Secure causes double-digit conversion losses. Being redirected to a new third-party website that is asking the consumer

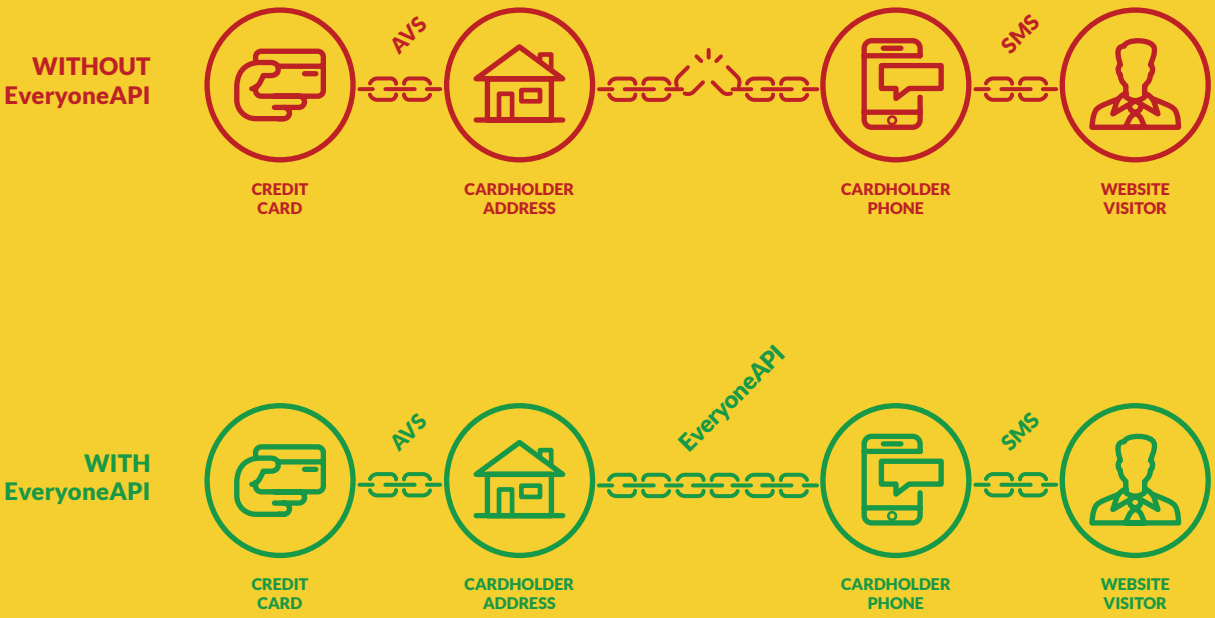
Verified by Visa and Mastercard Securecode or 3D Secure

for an additional password is a confusing hassle for consumers. Entering social security numbers to complete otherwise simple transactions creates discomfort and often leads to cart abandonment.

Merchants hate 3D secure

Merchants hate that they have no control over the third party web site for 3D Secure and the user experience at that site. Merchants who invest tens of thousands of dollars in creating an excellent user experience rightfully have no desire to send customers to extra websites whose branding and experience standards don't match their own. While merchants can sometimes benefit from a liability shift by using 3D Secure, this benefit is seldom realized due to the fact that very few chargeback reason codes are eligible.

The Effective Method for Identity Verification and Fraud Mitigation



We have seen that neither AVS, IP Geolocation, nor 3D Secure are adequate fraud deterrents when used alone. However, when AVS and EveryoneAPI are used in tandem, it is possible to mitigate nearly all online fraud.

AVS is an effective mechanism for tying a billing address to a credit card number. To mitigate fraud, the merchant must also tie the visitor on its site to the billing address. Without tying the customer to the billing address associated with the credit card being used, there is no reliable way to know whether the customer is the actual card holder.

The process for doing this is simple:

1. When the customer places an order or creates an account, the merchant asks the customer for a phone number and sends a verification code to the customer in an SMS text message or via a phone call. This is to verify that the customer has supplied a phone number which genuinely belongs to the customer.

2. Once the code is verified, the merchant uses EveryoneAPI to retrieve the address associated with the phone number.

3. If the address retrieved using EveryoneAPI matches the address supplied by the customer, then the merchant retrieves a payment authorization and AVS response from the payment processor.

4. If the AVS response is a match, then the merchant can now safely process the order with nearly absolute assurance that the transaction is not fraudulent.

This process may be employed for all transactions, one per new account, or only when a transaction has been identified as being high risk, at the merchant's discretion.

Unfortunately many providers of data available to card-not-present merchants and payment processors have very low coverage and don't reliably tie phone numbers to names and billing address. However, EveryoneAPI uses authoritative data sources and offers industry-leading data coverage that is relied on by payment processors, law enforcement, telephone companies, and online merchants alike. Without this coverage and a method of verification, merchants are significantly more susceptible to credit card fraud.

There are no monthly fees or long-term commitments associated with the use of EveryoneAPI. The time required to implement this solution is minimal, and the benefits can be realized immediately thereafter.

Conclusion

For too many merchants, online transaction fraud is far too real and devastating. Fraudsters are constantly working on new techniques to hone their craft which is why Telo is dedicated to providing merchants with tools like EveryoneAPI. It is essential that you take advantage of these tools to protect your business as carefully and strategically as possible. By protecting your business today using EveryoneAPI, you can prevent becoming another statistic in the war against online transaction fraud.

About Telo

Telo serves data to thousands of customers across many business verticals. From Caller ID for telephone carriers to fraud mitigation and compliance for financial service providers, Telo APIs are at the core of many business operations.

Schedule an appointment with a business specialist
Phone: 1-888-315-TELO (8356)
Email: sales@everyoneapi.com