Electronic DNA (eDNA™)
Identity and Reputation Based Risk Management

Background

Payment systems have evolved with the Internet. The credit card payment network supports varieties of transactions for e-Commerce, with the majority being "card-not-present" (CNP), where no physical card is actually presented at the time of payment. With CNP transactions, instead of taking the card information from the card itself, the card information is input by the customer to a merchant's payment application, which submits it through a payment gateway to the appropriate card network for funding. The payment method might be a credit card, debit card, gift card, pre-paid card, e-wallet or one of an increasing mix of mobile payment methods.

The merchant largely carries the financial liability for fraud in CNP transactions. To mitigate the risk, e-Commerce merchants send additional data through the payment gateway that the backend processors use to assess the risk associated to a given transaction. The data that is sent across is compared with data held by the issuer as well as the processors. Besides the card number, this typically includes the registered billing address for the card (enables Address Service- AVS check from the issuer), the Card Verification Value (enables CVV/CVV2 check from the issuer) number on the card, the expiration date, and often some other personal information such as name and phone number of the card owner. The response from the issuer to the request indicates which information matches and which doesn't and whether the issuer is willing to fund the transaction.

Banks reject transactions which they know or suspect to be fraudulent, or where there are insufficient funds to cover the transaction amount. Banks suspect there is fraud, for example, when the AVS, CVV or expiration date, are wrong. However, errors in other data, like billing address, aren't necessarily considered suspicious enough for the bank to reject the transaction. Fundamentally, the risk assessment is based on whether or not a small set of the data presented matches the data associated to the credit card that is stored at the issuer. Unfortunately, most of this data can be easily obtained in many Internet sites at a very low price, or it can be stolen where the card is processed outside the consumer's control: like a restaurant, retail store, fraudulent web site, etc.

In essence, even if there are no data errors, merchants cannot be sure that it hasn't been stolen and used in their online store. Since the merchant is liable for the final decision and any refunds or fines related to fraud, they must employ technology and best practices to minimize the chance of accepting fraudulent transactions from stolen cards and the corresponding losses.

The State of Anti-fraud Technology

Merchant anti-fraud technology for e-commerce transactions has emerged as a fast growing market in the payment industry. The technology is designed to supplement the existing anti-fraud services from the issuers and card brands by providing information and analysis on collected data from the consumers' online environment (e.g. connecting device, IP address geolocation, email address, etc).

In general, the different technologies identify anomalies in the data presented and the payment process and allow the merchant to either reject the transaction before submitting the payment to the bank or to reject it before any product is shipped. In the latter case, any transaction that was approved would have to be cancelled, leaving the merchant with the expenses related to processing and cancelling a transaction. In the former case, the major risk is making a mistake in cancelling a transaction and potentially both turning away a legitimate payment and also alienating a customer. Merchants frequently build "black lists" to capture the decisions which are made through their systems. This allows them to effectively ban the fraudulent cards. Nevertheless, there are still basic problems with the overall state of these solutions:

- Black lists provide very limited value.
- There isn't a clear way for merchants to share fraud data.
- Nobody is looking at systemic fraud in real time.

Let's review these in more detail:

Black Lists provide limited value

Much of the technology is built on the assumption that users can be identified by their computers: either through the computer's IP address or a computer/browser fingerprint - known as "device fingerprint". When and if fraud is proven, merchants would then add them to "black" or "banned" lists, effectively denying subsequent transactions associated to the banned or blacklisted devices. This denial of known bad entities is the basis for a large portion of the anti-fraud technology currently available on the market.

Many merchants build their own anti-fraud systems that track bad users. The most sophisticated merchants track bad users through cards, devices and IP addresses. Users may get flagged when their transactions are later charged back or when the merchant issues a credit to their card in order to prevent the chargeback costs and penalties. Even though this limits the exposure from those IP addresses or devices, device fingerprint technologies is easily circumvented, and blacklists do not prevent the initial fraud that was responsible for the refund or chargeback.

Looking at reputation databases of known fraudulent cards, IP addresses or devices is often too late. The merchant that is hit with a chargeback or loss through a refund probably suffered the major and perhaps only effect of that fraud incident. All negative systems are a step-behind. The goal is to prevent the first instance of fraud.

There is no infrastructure to share data

When card data is stolen it may get used at one or more merchants. A fraudster might create a single account at a merchant and use the card until it is discovered. Or, they might create similar accounts at multiple merchants and use the same card at those merchants - fraudsters have little risk of being caught or discovered. To those merchants, the accounts' seem good since the personal and billing information of the accounts match the data associated with the registered cards (it is part of the stolen card information).

When an issuing bank discovers a card is stolen, it will be cancelled. In contrast, if a merchant has a suspicion that a card has been stolen, the transaction will simply be rejected, and the card being used still be active and can be used at other merchants. When merchants suspect fraud, there are few mechanisms for them to verify or report it. The lack of visibility across the entities involved in transactions is a key problem in performing efficient anti-fraud.

No one is looking at Systemic Fraud in Real Time

Fraudsters have continued to evolve at incredible speeds – most instances of fraud are not isolated. For example, recent attacks on the net have utilized "botted" computers, computers that have been broken into and which can be controlled remotely. In those cases, the identity of the machine and the user cannot be verified by historic data. For all practical purposes, the transaction appears to be coming from a new user, a new card and all the information presented is correct. Detecting a botnet attack requires a different perspective than the one a merchant has.

Recognizing Identities in Transactions

The basic question of anti-fraud for the merchant is whether or not to submit and honor the transaction. If the merchant can verify the ownership of the card as belonging to the participant in the transaction, the risk becomes equivalent to the risk in a card-present transaction, which is much less likely to be fraudulent. The merchant will still hold the liability for the transaction since it is CNP, but with much less risk.

Relationships with customers are precious to merchants. Customer acquisition and retention is essential to all retail business and especially on-line businesses with the competitive nature of E-Commerce. Asking questions or forcing authentication is a sure way to lose business - customers are reluctant to give private information to new merchants given the potential for misuse of that information offering up personal information to a new website may very well be the method by which the new site steals the personal information. Technologies that can accurately identify customers in their transactions, respect their privacy and protect their identities are essential to efficient E-Commerce

IdentityMind has developed a patent-pending technology that identifies Internet users without introducing intrusive steps. IdentityMind's core technology **eDNA™ (electronic DNA), recognizes users through their Internet environment, payment data and payment behavior. It identifies good and bad users and provides tools to recognize when identities have been stolen.** With eDNA™ a user can be known from different devices, different IP addresses, using multiple payment instruments and even when they have different account names and email addresses. Identities are unique and each has its individual eDNA™.

IdentityMind eDNA™ (Electronic DNA) and Risk Management

eDNA™ solves significant problems for risk management operations: When a user is recognized, the decision of whether to accept a transaction or not is simple. It becomes an issue of business rules, rather than anti-fraud technology: Whatever reputations have been established can be utilized; If a user's identity has been compromised, it will likely be detected and the user can be notified and protected; If fraudsters attempt to exploit promotions or commit fraud through identity theft of existing users, they will be discovered. Protecting customers' identities and reputations, approving their charges and catching identity theft is all in merchants' best interests.

When a cardholder is recognized through their eDNA™, there is no question of ownership of the card and the fraud policy becomes very simple: if it is a normal transaction, just take it! There are no other questions; If the user has been a problematic one in the past, such as having contested purchases as not being theirs, then the transaction might be rejected or reviewed through a manual review process. Even a subset of the total available eDNA™ can be enough to remove doubt about the identity of the correct ownership and user of the card. The time and effort to evaluate the transactions as well as the false positive rate can be dramatically reduced.

eDNA™ catches fraud for merchants beyond transaction approval and analysis. When a merchant is hit successfully, fraudsters often collaborate and create multiple accounts to steal from the same merchant - they exploit known vulnerabilities. Similarly, if a fraudster is banned, they may try to come back as a new user and register under a different name with a different stolen card. eDNA™ detects these cases.

eDNA™ and the Current Anti-fraud Solutions

When fraudulent users are found, their eDNA™ becomes known. A merchant can use this information to protect against fraudsters coming back to their site under different account names. eDNA™ shows the relationships between users and transactions. A great deal of value is derived through comparing the eDNA™ for new and existing users and known fraudsters. It is with this use of identity and "electronic DNA" (eDNA™) that the problems with blacklists, systematic fraud and data sharing that were described above can be substantially improved.

Improving the Value of Blacklists with eDNA™

The problem with blacklists is the ability of fraudsters to hide their identities. For example, if an IP address is listed, a fraudster can come in through a proxy server or from a different compromised host circumventing any IP restrictions. This is the same for nearly every attribute. A card being blacklisted will always stop an actual owner- this is essentially useless in many cases. But a fraudster who uses stolen cards can come back with another card from another host that has not been seen before.

The value of blacklisting changes when users' eDNA™ is used for blacklists instead of individual attributes. eDNA™ holds the relationships between the identities involved with the different card when the eDNA™ is recognized, different cards and accounts are recognized as related. On the flip-side, the positive users are seen across their different computers, environments, cards and enjoy the positive reputation that they have within and across merchants. This is similar to "white-listing" a user. But, with the very substantial difference: With a "white-list", the transaction will immediately be approved without anti-fraud scrutiny; with a reputation built on postive eDNA™, any anomalies will be recognized as they occur: potential identity theft is discovered, and the potential fraud prevented.

Data Sharing with eDNA™

The problem with data sharing is the problem of protecting private information. Both merchants and customers can be affected when private information is shared. This applies to business practices as well as privacy laws that are becoming increasingly stringent. What is needed is a service that can effectively share fraud information between merchants without compromising the privacy requirements of customers or the merchants' business practices or customer base.

The use of eDNA™ across merchants provides the benefits of sharing data across merchants without introducing the problems of data sharing and compromise of privacy. The use of eDNA™ is analogous to the basic presentation of a card from the merchant to the payment processor; if the card is good then it will be approved and otherwise not. With eDNA™, if the identity is recognized as the real one it is acknowledged, otherwise it is not. This provides a private and secure method for all merchants to check whether a card is actually owned by the submitting user - it is the missing link in anti-fraud. eDNA™ does not show any private information. Instead it matches against presented information to recognize users and entities that it has seen before.

Recognizing Systematic Fraud with eDNA™

Systematic fraud is emerging as one of the major threats to E-Commerce. When fraudsters find merchants who are vulnerable, "botnets" can hit those same merchants with many transactions in matters of seconds. The cost to the merchants can be enormous as they may lose goods and money, suffer chargebacks and refunds. The effect can be similar to a denial of service on the merchant: good orders have to be filtered from those that are involved in these attacks, making everything more complicated and expensive.

As part of eDNA™, the recognition of commonality between transactions is fundamental: transactions are related through their common electronic DNA - shared eDNA™. Seeing that transactions and users are related can identify a systematic attack within and across merchants. When a systematic attack is detected through shared eDNA™, all the merchants who are effected are made aware of the attack and all the connections between the transactions, users, accounts, cards are made visible. eDNA™ enables an effective workflow that helps to limit the scope of systematic attacks and allows merchants to effectively detect and manage instances of the associated fraud.

Conclusion

eDNA™ provides a complete and sound risk management solution. It addresses the fundamental problems with the current anti-fraud and risk management technologies for CNP transactions: To recognize Internet identities and know whether the customer is authorized to use the given payment instrument. In addition, eDNA™ verifies the identity of the users without changing the flow of the transaction so merchants can be confident that higher security doesn't translate into consumer abandonment.