ThreatMetrix

WHITEPAPER

How Device Identification Defeats Online Fraud Whitepaper

- Verify New Account Originations
- Authorize Payments and Transactions
- Authenticate User Logins

Overview

The Internet makes it fast and easy for people to connect with other people, to buy things, move money and engage anyone anywhere in the world instantly. Before the Internet, fraud was mostly a paper-based scheme like check kiting, embezzlement, and forgery. But the benefits that the Internet offers businesses and consumers are also available to fraudsters: speed, global reach, efficiency, convenience—with opportunity, accessibility and anonymity that have made fraud a top concern for consumers, governments and businesses everywhere. Like the dog in the famous New Yorker cartoon that tells the other "No one can tell you're a dog on the Internet," it's very hard to tell if the person at your website is who they claim to be.

The doors that provide entry to good customers online are the same doors that fraudsters use to gain entry: logins, new account registration, and online purchases (card not present). The keys that enable people to pass through these doors are credentials, identities, account numbers, credit cards and personal information. Cyber criminals steal this information by tricking unsuspecting consumers into giving it to them unwittingly, or using technology to silently take over their computers and impersonate them or capture their keystrokes.

Profile the Device

Supposing you could tell whether a visitor to your website was more likely to commit a fraud or conduct a legitimate transaction before you had any personal information such as their account number or name. Just imagine the positive impact on your business. It's all made possible using a sophisticated technology called Device Identification. Device identification from ThreatMetrix profiles the computer instead of the person visiting your website. It's the impersonal side of personal computers—the operating system, browser, Internet connection and more—that enables device identification to help you decide whether to proceed, challenge or prevent a web transaction.

Device identification is made possible through advances in computer capabilities that make use of stores of both static and dynamic data managed by browsers, operating systems, and Internet connections to perform their work. The data available from these sources is sufficient to establish a unique 'handle' for a visiting computer to be referenced and recognized on the worldwide web. These data also provide insights that help you decide whether (or how much) you should trust a computer visiting your website.

Device Identification: A New Way to Detect Online Fraud

There are three ways to detect online fraud. Each relies on a different source of information: check the person, watch what they do and profile their computer. All are valuable and ideally all three should be used together.

Check the person (personal history)

When you have personal information such as a name or account number, a quick reference to Prior Account Activity Records and Credit History databases will enable you to assess risk based on what you know about them. The drawbacks to using PII (personally identifiable information) are 1) users reluctance to provide them (e.g. they don't trust your website) and 2) if a fraudster is using stolen identities or credentials they can in effect "be you" online and gain authorized entry.

Watch what they do (personal behavior)

Technology that monitors what a person does after they have gained access can provide useful insights that help you decide whether to trust the person to continue transacting. Here again, if a fraudster successfully gains entry using lost or stolen credentials they're already "past the front gates."

Profile the computer (device identification)

Collect anonymous information from a visiting computer and its connection to the Internet to reliably identify the computer and assess its risk. When many device characteristics are drawn from multiple sources in the computer and analyzed, they reveal hidden truths that help determine risk. Device risk, measured in seconds, delivers a valuable measure of risk with or without historical and behavioral anti-fraud tools.

How Device Identification Helps Control Online Fraud

There's more to device identification than the initial risk assessment based on what the computer's characteristics reveal through anomalies. Once you can reference computers (or mobile phones, iPads, etc.) visiting your website by their unique machine identities—also called their device fingerprint—you can see fraudulent patterns and behaviors linked to a computer that might otherwise go undetected. IP addresses are an often-used but undependable "handle" many companies employ in an attempt to link activity to individual computers. But IP addresses are unreliable because they can be shared by many computers or hidden behind proxies that mask the true IP address and thereby hide the true geo-location. A computer's fingerprint gives you a powerful perspective to see activity on your website in a new light that helps you detect—and stop—fraud.

Volume: Fraudsters use computers in ways that legitimate web visitors don't. For example, an abnormally high volume of transactions originating from a single computer using multiple credit cards and personal information is a telling indicator to risk.

Transactions: You can use a computer's device fingerprint to group transactions from a single computer over multiple visits to your website, or group transactions by characteristics such as the ISP and location.

Accounts: IP addresses can be shared or spoofed whereas the computer's device fingerprint quickly reveals when someone's lost or stolen credentials are "making the rounds" on the Internet for others to abuse. Device ID enables you to validate users or restrict access to subscriptions and hosted applications.

Device Reputation: The device ID can be used cross-reference a match in a shared list of device fingerprints and corresponding reputation information built on the experience of others who have submitted and flagged them based on suspicious or fraudulent activity.

Increased Automation: The advent of botnets and fraud tool kits provide an evolving and ever ready fraud threat platform, allowing fraud attempts to be spoofed from nearly every geography and computer network.

Even without a pandemic doomsday scenario, it's clear that the threat is real and very present, and the burden should not rest solely on the shoulders of fraud prevention and loss prevention staff because fraud management is not just about loss prevention, it is strategic to the operations of most major online businesses today.

Eight Advantages To Device ID

- Stop fraud before it happens. The computer reveals risk before the person—so you can decide whether to accept, challenge or reject within seconds.
- No personal data required. You don't need to wait for or rely on information about the person to detect fraud or recognize a customer because device ID uses anonymous computer characteristics.
- Returning computers are verified instantly by the unique characteristics of their computer. Instant validation that's entirely transparent to your customer enables better and smarter delivery of online services.
- Block returning fraudsters already flagged. The ability to instantly identify returning fraudsters by their computer enables you to block them from entering your website.
- More convenient and less risk to customers. The use of device ID can add an additional form of authentication that does not rely on personally identifiable information (PII) and passwords for verification. Fraudsters can steal (PII) to impersonate someone, but they can't steal a computer's unique device identity.

- No prior history required. Even without prior contact with a computer visiting your website for the first time, its anonymous characteristics give you insights that help you detect fraud.
- Increases effectiveness of other anti-fraud tools. Device identification is a powerful addition to home-grown and off-the-shelf anti-fraud tools. Device risk adds context to make better decisions more quickly.
- Effective for all three entry points on a website where fraud can occur: logins, new account registrations and online payments.

Conclusion

The motivation, means and opportunity for the bad guys to commit online fraud put increasing pressure on consumers and the companies they engage with to do more to prevent fraud. Consumer concern for becoming a victim of online fraud when they're banking, shopping, networking with friends or dating is on the rise thanks to a constant drumbeat of warnings to protect their online identity and Internet scams reported in the news. Consumers can and will shoulder only so much of the burden to protect themselves—they expect their providers to employ the latest technology that will keep them safe. Device identification can help manage risk earlier in online transactions by detecting fraud sooner and providing customers a better online experience. ThreatMetrix device identification offers companies a proven device identification technology with distinct advantages that deliver smarter, faster and more affordable device-based risk management.

For more information, please visit us at:
www.threatmetrix.com

V1.10.2013