AUGUST 2018

Why Device Age Matters:

Retaining device history for more than 6 months can save millions in fraud losses

iovation®
A TransUnion® Company

You may have heard that storing device data for more than a few months has no incremental value in preventing fraud and abuse.

Or that it doesn't matter because fraudsters frequently change their devices.

When you hear these arguments from a device-intelligence vendor, it may mean they:

- Want to avoid the cost of storing device data for more than a few months
- Cannot access and analyze more than a few months of data in real time
- Can only report on device risks, not device reputation

In case you aren't familiar with the term 'device reputation', it's a history of confirmed details on fraud and abuse for a specific device. These are specific details that have been reported by a fraud or security analyst at companies like yours.

What if a device visited your online property and you knew that it had been reported as involved in identity theft, credit card fraud, and credit card application fraud? Even if all other aspects of the device seemed normal, that history would make you hesitant to do business with the device, wouldn't it?

This is why maintaining device data for extended periods of time is used to help prevent fraud. In fact, this unique capability is so useful for iovation's customers that 59% of the transactions they reject are due to the device's reputation. This means a better fraud catch rate for you and less false positives!

Introduction

Web-connected devices that have been involved in fraud or abuse are more likely to be involved in committing fraud or abuse in the future. Seems like a self-evident truth, doesn't it?

Believe it or not, some would have you believe that keeping a device's history – for more than a few months or even a year – does not materially impact a company's ability to identify and catch more fraud.

Cybercriminals will use any and all devices available to them in order to lie, cheat and steal from you. Until they're blocked. Then they switch to different devices, counting on your fraud prevention efforts to forget about their old devices. When that happens, they start using their old devices again. They would love for you to believe that device history isn't important.

That's why your fraud prevention tools shouldn't forget older devices either. It's essential to know when a device, especially one that's new to your business, has a history of fraud. Even if that fraud happened years ago.

In this short report, you're going to learn:

Why device reputation is essential in the fight against online fraud and abuse.

Why it doesn't matter if cybercriminals change devices over short periods of time.

Why that other school of thought wants you to ignore device history past a certain point.

Importance of Device Risk History

iovation starts tracking device risk information the first time it appears on our network, as a result of it visiting one of our customers' web or mobile applications. From that point on, if this device visits any of our customers' online applications, we will contribute to that device's risk history.

You might wonder what type of data we are able to read from a device. Hundreds of different attributes allow us to uniquely recognize the device by constructing a 'device fingerprint.' In addition, these attributes enable us to identify risks associated with the device. For example, we can tell if the device has been compromised from jailbreaking or rooting, if certain attributes aren't consistent with the device type, and assess the likelihood that a device is providing an accurate IP address or if it is being spoofed.

This type of device-based risk assessment is not unusual as most device intelligence vendors offer a similar capability. However, there are three aspects about what iovation does that makes our solution unique. First, we do not obtain or store directly identifiable personal information (such as names or physical addresses) of the person using the device, so we have no way of knowing who the individual is behind the device (important for privacy concerns). Second, not only can we recognize the same device at a future point in time, but we are also able to do so as the device moves between different businesses and industries (important for tracking device history). Third, our patented device and account mapping capabilities enable us to construct associations between related sets of devices (important when fraudsters are using multiple devices).

These last two items enable us to offer a highly effective and unique fraud prevention feature known as device reputation. Device reputation, sometimes referred to as device risk history, is the list of confirmed cases of fraud or abuse associated with a device.

Here's how device reputation works. When one of iovation's customers confirms a case of fraud or abuse, they file a reputation report with our network. If this device later visits the same customer or any other iovation customer, the customer is immediately notified of the past history of fraud.

Most device intelligence vendors store device data for 30 to 180 days. Without a device reputation capability, there is little reason to store device data longer than this. But, with device reputation information, it becomes critical to store data for longer periods of time.

iovation keeps device reputation information for at least two years from the last transaction that occurred on our network. If the device has been involved with confirmed fraud or abuse, we will keep the device reputation information for at least five years from the last transaction.

"Five years?" You may be thinking. "That's an eternity on the web. Don't people upgrade their devices every 18 months on average? If so, why store the data for so long? Also, what about fraudsters? Certainly fraudsters must know that their devices will eventually get blocked. Don't they just pitch them out and replace them with new devices?"

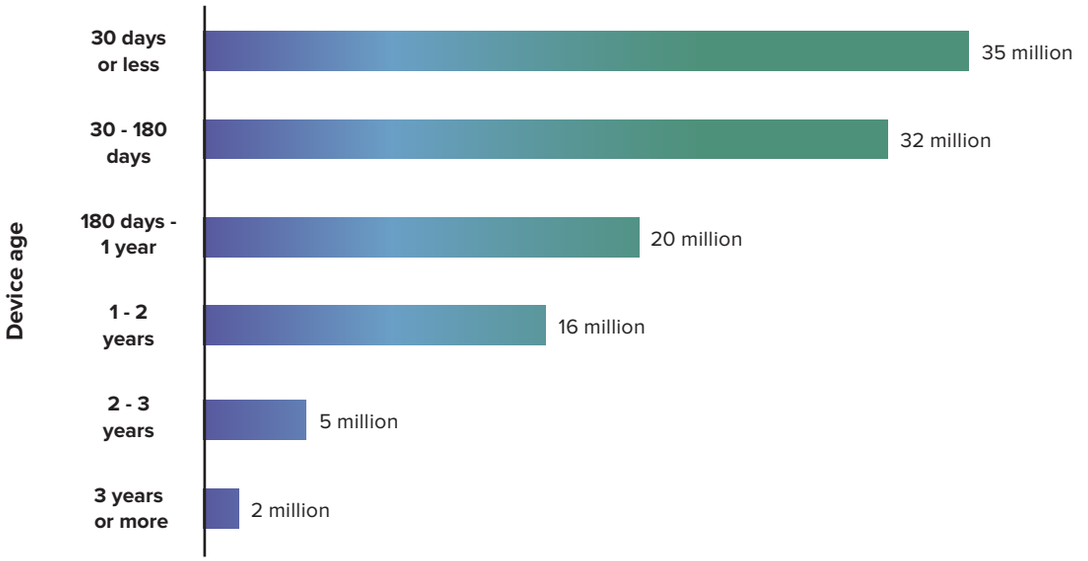
In this report, we'll look at data that explains why device history is not only relevant but is also extremely valuable in fighting fraud.

The first question that we're going to address is if the industry myth is true that devices 'disappear' after just a few months. Then we'll address the fraud prevention value of storing this data for extended periods of time.

FIGURE 1

Transactions by device age

Number of transactions (sampled over a one week period)



About the data used in this report

This report uses a representative sample of iovation transaction and device data from a one week period during May 2018. 110 million transactions were analyzed for this report.

Each transaction in this analysis involves a specific device. When we use the term 'age of device' or 'device age', what we mean is the elapsed time from when iovation first sees the device on our network to the date of the transaction included in this analysis. For example, if we say the age of a device is between '180 days to 1 year', that means that we first saw the device on our network between half a year and 1 year ago. Age of device refers neither to the device's physical age (date of manufacture) nor how long a particular consumer has owned the device.

In Figure 1, we can see that during this 1 week period there were 16 million transactions processed that involved a device with an age between 1 year and 2 years, and 5 million transactions with a device age between 2 years and 3 years.

Do Devices 'Disappear' After a Few Months?

Common sense would lead us to predict that old devices indeed eventually get replaced by newer ones. But, when does this drop-off occur? Six months? 18 months?

Figure 1 shows the number of transactions that iovation processed in a one week time period grouped by the age of the device used in the transaction. As can be seen, there is the expected drop-off in the number of devices as the device age increases. But, there are two interesting things to point out.

First, 43 million transactions, **in just 1 week**, involved devices that were at least 6 months old, the age at which many other device intelligence vendors stop storing device data. Extrapolated out to one year, this means that iovation provides its customer with device insight on approximately two billion more transactions than our competitors can.

Second, even though the drop-off in volume is steep as device age moves beyond two years, it is not inconsequential. Seven million transactions were processed on devices that have a device age of at least two years. Extrapolated out to 1 year, this represents approximately 364 million transactions. These are transactions that iovation can uniquely provide reputation insight on: Do they have a history of fraud or no history of fraud?

Use Device Reputation for Smarter Decisions

Device reputation accrues over time. Every account creation, login, and transaction contribute. Trustworthy devices exhibit good behavior consistently.

For the purposes of this report, we're interested in devices that have committed fraud or abuse. If you receive a visit from an unfamiliar device, and it has a bad reputation, you want to know about it.

But you don't just want to know if the device has a bad reputation. You want to know the basis for that reputation in granular, confirmed detail.

If the device is unfamiliar, you won't have that insight. Device recognition by itself will show you attributes and actions. But not reputation.

We created the FraudForce Community, a global network of more than 4,000 fraud professionals, as a way to share information about devices involved with fraud and abuse.

When one of our users discovers that fraud or abuse has occurred, they tag the offending device with a detailed reputation report in our database.

We track several different types of fraud and abuse, ranging from credit card fraud to cheating at gambling to chat abuse. Every user is intrinsically motivated to add the highest quality of evidence to these reports. They all rely on these reputation report details to increase catch rates and decrease false positives.

These reports — now over 55 million — establish the reputations of the devices to treat with caution.

Every member in our network uses this insight in their decisions to approve, deny or review transactions. Out of the millions of transactions that our customers deny with our services, 59% are rejected due to device reputation.

If you aren't using device reputation, how many fraudulent transactions are you missing?

FraudForce network of more than

4,000

Fraud Professionals

More than

55 million

Reports

Transactions Rejected

59%

Device Reputation

Device Recognition Underpins Device Reputation

If you've ever bought a pre-owned car, then you've probably used a flavor of device reputation.

It's an event notorious for inducing stress. What if the car breaks down soon after the sale? What if the seller withholds information they know might dissuade you?

If you knew the car had a history of engine trouble or had been involved in an accident, you might not buy it. Even if it seemed fine during a test drive. Even if it passed a mechanic's inspection.

That's why vehicle history services have become so popular. They'll check the car's vehicle identification number (VIN) against their database. Their report may mean the difference between getting a great deal and buying an expensive problem.

The same principle applies to device reputation. It goes beyond standard factors most commonly used to assess risk, such as: "Is it coming from a risky geolocation?", "Has it been jailbroken?", or

"Are the device's attributes odd or inconsistent?" These questions are basic imperatives but do not give the most accurate picture of intent.

Device reputation depends on reliable and accurate device recognition. And the longer, the better!

iovation's device reputation goes well beyond what other device intelligence solutions are able to offer when they consider device risk alone.

Maintain Relationships Between Devices for Years

Earlier we mentioned our unique capability of building associations and connections between related sets of devices and accounts (accomplished without the need of directly identifiable personal information). This capability is extremely valuable when device reputation data is stored for extended periods of time. Consider this example: A fraud ring uses a set of devices to commit fraud. Eventually, they are caught and the devices they used to get blocked because an iovation customer has filed a reputation report. If the fraud ring switches to different devices, the device reputation history of the blocked devices will continue to be associated with their new devices, and thus, continue to thwart their efforts. This is another reason why iovation stores device reputation history for extended periods of time.

Track Device Age for Years to Fight More Fraud

At the start of the report, we said we would answer the question of whether storing device data for extended periods of time was effective in fighting fraud. In this section, we'll do just that. Some people in the industry argue that maintaining device data for more than 45 days isn't worth the cost of storage. They are considering device age only as an attribute of device risk. We believe that's shortsighted.

We see devices with histories of fraud and abuse still attempting transactions for years after our first encounter.

They don't know who our subscribers are, so they keep trying. Perhaps it's because they've been successful on websites and apps that don't use iovation services. iovation customers see a device's reputation in real time. They know the reputation report came from one of their fraud-fighting peers in our network.

FIGURE 2

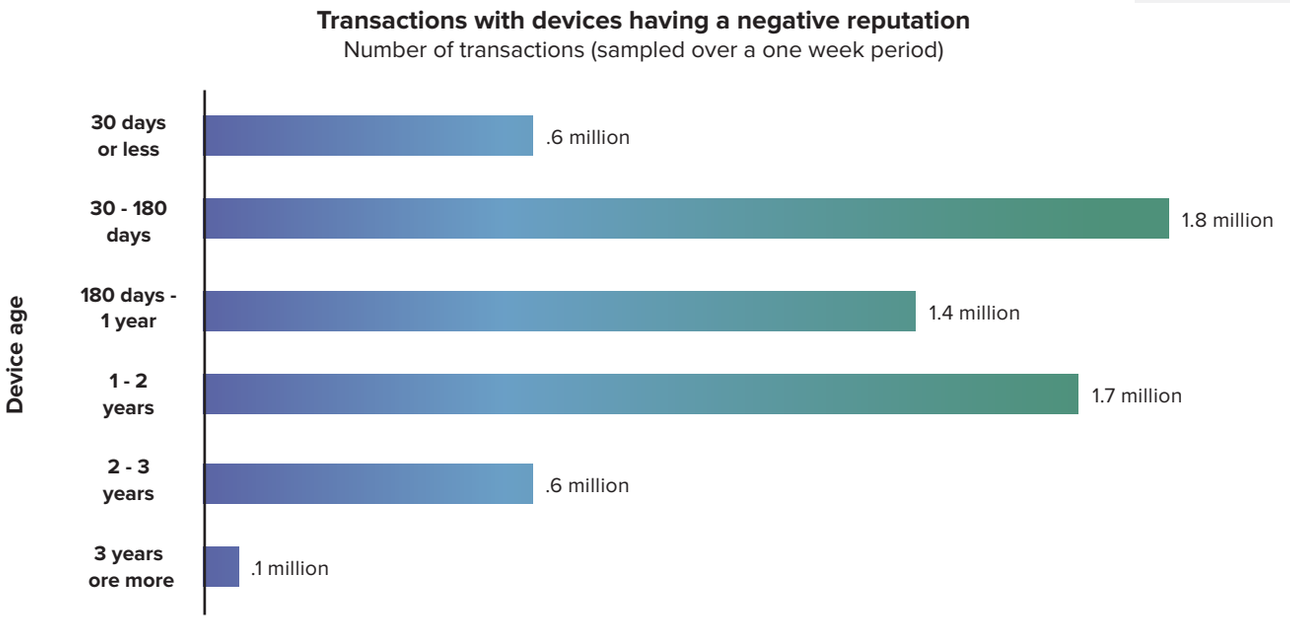


Figure 2 shows the number of transactions involving devices that have a risky reputation (meaning that an iovation customer previously reported that the device was involved with confirmed fraud). This data shows that fraudsters continue to try to use devices, sometimes years after the first case of fraud is reported.

Nearly four million transactions were processed over just a one week period involving known risky devices where the device age was six months or older. Because of iovation's device reputation capability, we were able to warn our customers of the specific risks that these devices presented. Nearly 100,000 of these transactions involved risky devices that were 3 or more years old. Without the device reputation history, our customers would not have known of the potential for fraud from these devices.

Let's put this in the context of preventing fraud loss. Let's assume that each transaction iovation protected with device reputation history would have resulted in an average of $25 fraud loss. Then over a 1 week period, iovation protected our customers from potentially $190 million in fraud losses more than solutions that do not store device history for more than 6 months.

Risk of Known Devices Versus Unknown Devices

Even considering this data, some might argue that a relatively small number of total transactions involved very old (more than three years) devices with a history of fraud. However, as we know in fraud prevention, the unknown is risky whereas the known is much less risky. If two devices visit your online app and you know nothing about the first one but you know that the other one has five years of history with no reported incidents of fraud, which one are you more likely to trust?

Conclusion

Older devices are not riskier by default. As a device-risk attribute, age isn't important.

However, device history underpins an entire pillar of device intelligence: reputation. Reputation provides context absent from device recognition or behavior.

If you know the history of the device, you can ask smarter questions, such as:

- **Has that device committed fraud or abuse in the recent past?**
- **What is the relationship of accounts around that device?**
- **Is this device connected to other devices with bad reputations?**

If your device-based fraud prevention partner can't store device reputation for years, you can't ask these questions. They may argue the answers aren't important. Ignore them.

Reputation is ingrained in our culture and economy. Criminal background checks help to confirm that prospective employees' will make good hires. Credit histories help to confirm that borrowers will repay their loans. You use reputation in your own life to help determine whom to trust.

Fighting fraud is tough in today's world. As a fraud prevention specialist, you know that every effort counts. Many would consider lowering their fraud losses by 0.5% a great benchmark. iovation's unique capability far exceeds this. As the data shows, in just a single week's time, iovation helped our customers stop potentially four million transactions that involved devices with a history of fraud. This is because we understand the importance of storing device data for extended periods of time.

Shouldn't your organization include device reputation in its fraud prevention process, too?

ABOUT IOVATION

iovation, a TransUnion company, was founded with a simple guiding mission: to make the Internet a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multi-factor authentication methods, iovation safeguards tens of millions of digital transactions each day.

Global Headquarters

iovation Inc
555 SW Oak Street,
Suite #300
Portland, OR 97204 USA

PH +1 (503) 224 - 6010
FX +1 (503) 224 - 1581
EMAIL info@iovation.com

www.iovation.com

iovation®
A TransUnion® Company