Definitive Guide™

to

Next-generation Fraud Prevention

Fraud Prevention Techniques
for the Mobile Age

Crystal Bedell
Eddie Glenn

FOREWORD BY:
Scott Waddell

Compliments of:

iovation®
A TransUnion® Company

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.

Definitive Guide™

to

Next-generation Fraud Prevention

Fraud Prevention Techniques
for the Mobile Age

Crystal Bedell
Eddie Glenn

Foreword by Scott Waddell

CYBEREDGE
PRESS

Definitive Guide™ to Next-generation Fraud Prevention

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-0-9990354-4-3 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Special Help from iovation: Jim Hendrie, Thomas Lieberman, Joe Barstow

Table of Contents

Foreword

Fraud in today's world is much different than it was 30, 20, or even 5 years ago. The only constant being that where there is business opportunity, there are fraud opportunities as well.

Next-generation cybercriminals use many different tactics for committing online fraud. Massive breaches of personal information and login credentials have enabled them to commit wide scale account takeover as well as to easily assume the identity of millions of individuals. Fraudsters also use sophisticated technologies such as computer and smartphone emulators, machine learning, and bots to commit fraud at a global level, often simultaneously targeting hundreds of online businesses.

Next-generation fraud attacks require next-generation fraud prevention measures to stay ahead of cybercriminals. Advanced technologies such as machine learning and device intelligence along with collaboration across businesses to share fraud insights are effective at detecting and stopping online fraud. In addition, technologies such as dynamic authentication not only stop unauthorized access to an online account but also enable a frictionless consumer experience for authorized users of the account.

Even as cybercriminal efforts rise, consumer expectations for their online and mobile experience are as well. Consumers demand mobile access, from anywhere in the world, at any time. Consumers want a fast response time, be it the approval for an online loan application or an online purchase. Even though they resent cumbersome username/password login requirements, they still expect their accounts and data to be safeguarded.

This puts a squeeze on fraud prevention specialists. How do you balance the business need of fighting fraud with the market need of a great user experience? Next-generation fraud prevention solutions help with both.

iovation was founded in 2004 with the mission of making the Internet a safer place for people to conduct business. Since then, our next-generation device intelligence solution has protected over 35 billion online global transactions. Our network has seen over 5 billion devices ranging from desktop computers to smartphones to Internet of Things (IoT) devices and gaming consoles.

Our consortium of cybercrime fighters share fraud intelligence within our customer network. They have submitted more than 50 million fraud and abuse reports over the past 14 years, which have helped prevent hundreds of millions of fraud attempts. We are pleased to sponsor this Definitive Guide™ and hope that it will help you fight the next generation of cybercriminals.

Scott Waddell
CTO
iovation

Introduction

The digitalization of business processes and advent of mobile computing have given rise to the next generation of fraud. Cybercriminals have a variety of tools and techniques—as well as opportunities—to steal money and services. Furthermore, traditional fraud prevention tools often fail to stop this fraudulent activity.

Companies need a new approach to fraud prevention—one that stops fraud early and preserves the user experience. Companies with an online presence must have the ability to:

- ☑ Detect and respond to fraudulent activity before incurring losses
- ☑ Leverage human insight and machine learning to identify advanced fraud
- ☑ Work with other fraud analysts to identify larger fraud trends and stop cybercriminals on a global scale
- ☑ Block more fraud while reducing fraud prevention costs

This book explores how companies can leverage a next-generation fraud prevention solution to stop more fraud while reducing costs and providing a positive user experience for trusted customers.

Chapters at a Glance

Chapter 1, "Introducing Fraud in the Mobile Age," examines how fraud has evolved with the advent of anywhere, anytime computing.

Chapter 2, "Understanding the Enemy," explains how cybercriminals commit fraud, as well as the tools and techniques they use to do so.

Chapter 3, "Analyzing Current Fraud Prevention Techniques," describes how traditional approaches used to block fraud fail to counter today's next-generation fraud.

Chapter 4, "Introducing Next-generation Fraud Prevention," explains the tools and techniques that comprise a next-generation approach to fraud prevention.

Chapter 5, "Exploring Device Intelligence," introduces the concepts of device recognition, reputation, and associations for blocking fraudulent activity.

Chapter 6, "Leveraging Human Insight and Machine Learning," explains how human insight and machine learning are better together in the fight against fraud.

Chapter 7, "Harnessing the Power of Next-generation Device Intelligence," explores the benefits of a next-generation approach to fraud prevention beyond simply catching more fraud.

Chapter 8, "Ten Buying Criteria for a Next-gen Fraud Prevention Solution," enumerates criteria for choosing a next-gen fraud prevention solution.

The Glossary provides handy definitions of key terms (appearing in *italics*) used throughout this book.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

Introducing Fraud in the Mobile Age

In this chapter

- Learn why it's easier than ever to commit fraud
- Understand how your business is affected by fraud
- Explore the impact of fraud on your customers

The way we live, work, and play has been transformed by powerful computing devices that can fit in a pocket. Virtually any transaction you can do online can be completed faster, more easily, and more conveniently via a mobile device. Unfortunately, those same benefits apply equally to cybercriminals and fraudulent activity.

In this chapter we look at the state of fraud today and the impact it has on both your business and your customers.

Welcome to the Mobile Age

The Mobile Age is characterized by the ability to transfer information freely and quickly while on the go. This has significant ramifications for both businesses and their customers. By digitalizing processes, businesses can reduce operational costs. They can automate processes that previously required time and effort from personnel. Businesses are even digitalizing processes that were previously handled by the back office and making them customer facing.

For years, consumers have enjoyed the convenience of having services offered online. Transactions that once were conducted in person are now available on the web, and many

of these online transactions now occur on mobile devices. It's easier than ever to perform virtually any transaction, and from anywhere in the world.

Not only does the digitalization of processes give us location independence, but it also provides near real-time results for many transactions, or at least significantly decreased approval times. Loan applications can be approved in hours instead of days. Insurance claims can be processed in weeks instead of months. A store's merchandise inventory can be perused in minutes, and buyers can be immediately informed if some items are out of stock.

And then, of course, there's the introduction of new markets as businesses realize new revenue streams by making their services mobile. The gambling industry is a prime example. It has experienced phenomenal growth as customers enjoy the excitement and convenience of playing anywhere they have an Internet connection on their mobile phone.

But the Mobile Age is not all roses. All the benefits your customers enjoy due to the ability to easily and quickly transfer information are also leveraged by criminals. As businesses take more processes online and make them customer facing, they provide more opportunities for fraud to occur.

Fraudsters can do their dirty work from anywhere in the world. Instead of having to apply for a new credit card or bank account in person, fraudsters can hide behind the Internet's anonymity. In short, criminals can conduct fraud faster, more easily, and with less risk of getting caught.

At the same time, the tools and know-how needed to commit fraud are more readily available, lowering the barrier to entry for would-be fraudsters. For instance, fraudsters use the Internet to buy, sell, and trade victims' personal and financial information. They've also built thriving illegal networks to share data and techniques on how to defraud businesses. Literally, anyone, anywhere in the world can commit fraud in the Mobile Age.

The impact of fraud on businesses

The risk of fraud has exponentially increased in the Mobile Age. In addition to the reasons explained above, fraud rarely occurs as a single incident, but rather as a series of criminal acts. If not identified early, a single occurrence of fraud can lead to a multitude of other incidents.

Fraud impacts businesses in a number of ways:

- ☑ *Fraud losses* result when fraudsters directly steal merchandise, money, or services from a business. Examples of these losses include merchandise purchased with stolen credit cards, fraudulent credit card or loan accounts opened using stolen or synthetic identities, and payment of fraudulent insurance claims.
- ☑ *Revenue losses* can occur when fraudsters target special programs meant to grow revenue, such as promotions. For example, if an e-commerce business wants to attract new business by offering a 25% discount to the next 100 new customers and this offer is used by fraudsters instead, the company will not be able to meet its goal for the promotion.
- ☑ *The cost of fraud prevention* rises as fraud attacks increase. It's generally cheaper to stop fraud before it occurs than to try to recover fraud losses. In addition, when suspicious accounts or transactions are flagged for deeper investigation, organizations experience operational inefficiencies and higher costs. Oftentimes, manual review requires additional personnel to handle calls, manage records, and analyze applications or transactions.
- ☑ *Customer attrition* is also a problem when businesses are affected by fraud or fail to streamline their fraud prevention measures. Once a customer experiences a financial loss as a result of online fraud, retaining that customer becomes incredibly difficult. Any experience with fraud can increase customer attrition and revenue loss.

  Unfortunately, if organizations aren't careful, their attempts to counter fraud can actually increase customer attrition. As more controls and checks are added, they create a larger barrier to entry and diminish the user experience.

- ☑ Organizations that struggle with high fraud rates suffer the fallout of a *tarnished reputation*. In addition to increasing customer attrition, a damaged reputation can make it difficult to establish and renew contracts with business partners. Stakeholder and investor trust may erode. Plus, the organization becomes an attractive target for future fraud attempts because it is seen as deficient in protection.
- ☑ *Legal penalties* could result for businesses that are found negligent in preventing fraud. They may be liable for regulatory compliance violations, such as federal fines and payouts to customers whose identities were stolen.

The impact of fraud on customers

Businesses have the resources to help mitigate fraud, but customers, oftentimes, do not. A single incident of fraud or identity theft can have significant ramifications.

- ☑ Customers incur *financial losses* resulting from the incident itself. If they're lucky, and they recognize the fraud attempt, they can recoup the funds by filing a fraud claim with the impacted business. However, doing so results in…
- ☑ *Loss of time* as customers work with the various parties involved: retailers, credit card providers, financial institutions, etc., to file a fraud claim and wait for it to be reviewed.
- ☑ If the customer isn't aware of repeated fraud attempts or identity theft, the criminal activity can result in damaged *credit*. Depending on the extent of the damage, it could take years for a customer to recover.
- ☑ Customers expect the institutions and businesses they work with to secure their data and prevent criminal activity. A single incident can create bad *feelings* that end an otherwise mutually beneficial relationship.

Chapter 2

Understanding the Enemy

In this chapter

- Learn the difference between first-party and third-party fraud
- Examine the three categories of fraudulent activity
- Understand the tools and techniques cybercriminals use to defraud organizations

As we explained in Chapter 1, the Mobile Age provides ample opportunity for fraud. This fact, combined with complex schemes to circumvent conventional methods of fraud detection, is driving the need for a next-generation approach to fraud prevention.

But before you can effectively fight fraud in the Mobile Age, you must understand what you're up against. In this chapter, we take a look at the adversary. By understanding the tools and techniques cybercriminals use in their attempts to commit fraud, you'll be better prepared to combat them.

Understanding Next-gen Fraud

As we mentioned in Chapter 1, the digital exchange of information lowers the barrier to entry for professional and aspiring cybercriminals. There are many different ways to commit fraud and many types of fraudulent activity.

First-party fraud

An individual who commits fraud in their own name using their own account information commits *first-party fraud*. For example, in banking, first-party fraud occurs when an

individual takes out a loan or credit card in their name with no intent to ever repay the debt. In the insurance industry, quote manipulation is another form of first-party fraud. It occurs when a person submits false information, like the wrong home address, to receive a lower quote on the premium.

Third-party fraud

Third-party fraud occurs when either an individual or a group (like a fraud ring or a state-sponsored cybercriminal organization) does their dirty work under someone else's name.

The Internet serves as a conduit for the buying, selling, and trading of people's personal and financial information. Fraudsters use these stolen identities for multiple purposes. In some cases, they use the stolen identity to create an account or take out a loan in another person's name. Or, they may use stolen credentials to log into a person's online account, which is known as *account takeover*. Here, the victim is the individual whose identity was stolen. Oftentimes, the victim discovers this only after being denied a new loan or seeing that their credit score has dramatically dropped.

Another use of stolen identity is a bit more sinister, at least for a company that does business online. In this case, the fraudster does not use the stolen identity information of a single individual. Instead, they take bits of stolen identity information from various people, add completely fake information, and create an online identity for a completely new, but fake, person. This is referred to as a *synthetic*, or 'Frankenstein,' identity.

By mixing and matching real victims' actual names, addresses, Social Security numbers, and credit card details, fraudsters can create new identities that look legitimate. Synthetic identities are especially difficult for online businesses to detect in that there is no consumer 'victim' to report an unauthorized account. This fraud may go unnoticed for a very long time. It isn't until the account goes into arrears that the business realizes something is wrong. Even then, it's difficult to distinguish third-party synthetic identity fraud from a typical first-party loan default situation.

How They Do It

One of the reasons why it's difficult to identify and stop fraud today is because fraudsters have different modus operandi, depending in part on the type of fraudulent activity they're committing.

Categories of fraudulent activity

Fraudulent activity can be categorized into one of the following three groups:

1. Organized criminal or rogue state activity. Often committed by fraud rings, organized fraud involves a premeditated scheme to defraud others. In other words, it's carefully planned and executed to steal money or property from one or more victims. Organized fraud is a criminal offense.
2. Opportunistic but premeditated. Criminals create a scheme for committing fraud but do so when the right opportunity presents itself.
3. Opportunistic, spur of the moment. This final category of fraud is not premeditated. On a whim, when applying for a line of credit, a consumer inflates his salary, for instance.

Types of fraud

There are many different types of fraud, and they vary from one industry to another, as shown in Figure 2-1. To make things more complicated, fraudsters can work across multiple industries, leveraging the gains from one attack to execute another. Credit card fraud is often the entry point for all other types of fraud. For example, a criminal may apply for a dozen credit cards using unique synthetic identities, and then use them on retail websites. Next-generation fraud protection needs to target all types of fraud, across every industry—not just credit card fraud.

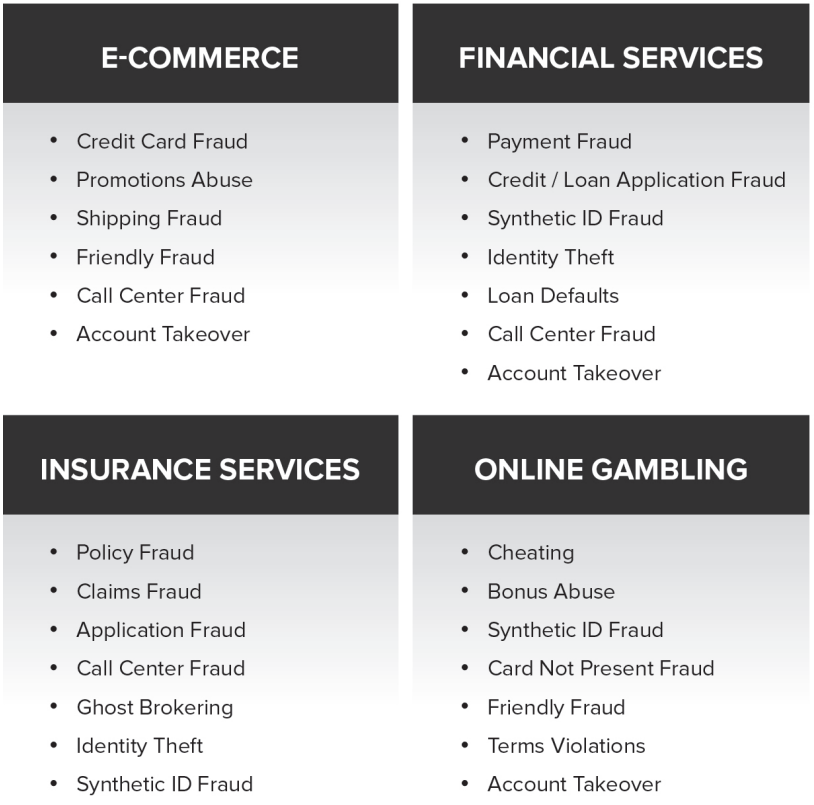


Figure 2-1: Fraud varies from one industry to another.

Anatomy of an attack

No two fraud attacks are identical. Cybercriminals have a number of tools and techniques at their disposal, which enable them to switch up their approach.

Tools and techniques

Cybercriminals are embracing new and increasingly sophisticated tools and methods to commit fraud. As a result of massive data breaches, criminals can purchase *personally identifiable information* (PII) and access credentials on the dark web. PII is information, such as name, phone number,

and mailing address, which can be used on its own or with other information to identify, contact, or locate an individual. As we mentioned previously, Internet-savvy criminals use this information to create synthetic identities that can circumvent conventional fraud detection methods.

Fraudsters have also been known to socially engineer attacks through call centers and in stores. *Social engineering* is the practice of manipulating people to trick them into disclosing sensitive information or do something they wouldn't normally do, like go against corporate policy. It is a non-technical attack that entails capitalizing on the human desire to be of help to others.

While social engineering is an age-old attack method, there have also been reported cases of fraudsters using newer technologies in their fraud attacks, such as sophisticated automated tooling and even machine learning.

Fraudsters also make use of a variety of technologies.

Common Technologies Fraudsters Use

Botnets are software programs that run on multiple computers in a coordinated fashion. Sometimes they infect a computer without the owner's knowledge. A central server, controlled by the fraudster, then uses this network of connected computers (bots) to coordinate attacks.

Emulators and simulators are software programs that pretend to be entirely different devices. For example, an iPhone emulator may run on a Windows machine, making it look like the transaction is coming from an iPhone. Unlike physical phones, emulated phones can be programmed to automatically target sites with attacks.

Proxy masking is when a fraudster hides their true IP address. When a computer or mobile device is part of an online transaction, its IP address is recorded. The IP address is useful for determining the location of the device. Fraudsters know this, and they use proxies to mask their true IP address. The most common proxy is *Tor (The Onion Router)*.

Machine learning is a form of artificial intelligence. It's useful in helping computer programs seem more human-like. Therefore, machine learning is useful for fraudsters to create synthetic identities and to control how their bots automatically attack online businesses.

Continual evolution of attacks

Because fraudsters continually change their tactics, fighting fraud is much like a bad game of "whack-a-mole." You might stop fraud in one place, only to have it pop up somewhere else. The trend toward omnichannel customer service only facilitates this problem. The moment an organization is successful at stopping fraud in one channel, the fraudsters move to another. This makes it impossible to stop all fraud. Organizations today must act quickly, be able to identify subtle trends, and recognize when standard detection methods don't work.

Simply put, organizations can't trust the information attackers provide. This drives the need to deploy more-effective anti-fraud solutions that look at information independent of the data supplied by users.

Like everyone else on the planet, fraudsters are dependent on their mobile devices, but they use them to commit fraud. They may also switch up devices and identities to evade detection. Even if a fraudulent account is detected and shut down, an organization that lacks the ability to identify fraudulent computers cannot prevent fraudsters from immediately creating a new account under a new identity. This creates a revolving door for repeated fraud and abuse.

Leverage the Internet

The nature of the Internet itself helps facilitate fraud. Cybercriminals leverage its built-in anonymity, scale, and complexity to circumvent identity- and financial-based fraud management systems.

The Internet also enables fraudsters to quickly move from one online business to another. Fraudsters may commit fraud with a financial institution by creating a new credit card, then test it on online gambling sites, and use it to make a purchase from an online retailer. Because of this type of pattern, it's critical for the entire online community, regardless of industry, to cooperate in fighting fraud.

Chapter 3

Analyzing Current Fraud Prevention Techniques

In this chapter

- Find out why business rules alone don't prevent fraud
- Explore the blind spots in a traditional fraud prevention strategy
- Understand the impact of your fraud prevention efforts on the customer experience

Companies aren't sitting idly by while cybercriminals steal their money and goods. Once fraud prevention teams understand how easily criminals obtain and alter PII, they attempt to do something about it. Unfortunately, they usually respond by adding more identity-based controls. These tools add customer friction, rely on even more personal information, and can leave organizations more susceptible to identity theft.

Because identity-based fraud prevention systems operate on identities, they often have difficulties tracking situations where identity is deliberately varied by fraudsters, making fraud detection in the case of stolen identity or synthetic identity more challenging. Furthermore, when fraud rings are committing fraud using hundreds of different identities, sometimes these cases appear isolated, which prevents businesses from connecting them as related incidents of fraud.

But that's just the start. In this chapter, we take a closer look at why a traditional fraud prevention strategy doesn't cut it in the Mobile Age.

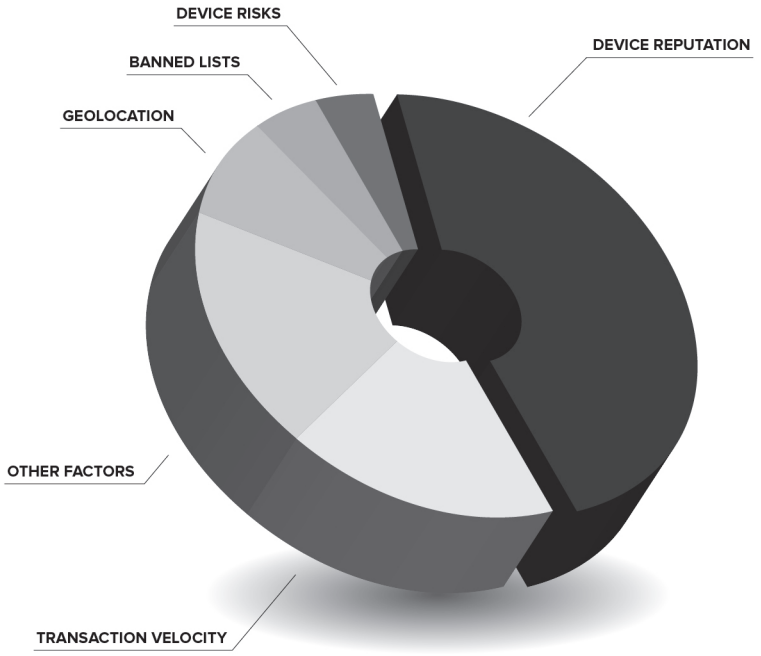


Figure 3-1: According to iovation, businesses blocked fraudsters for the above reasons in 2017.

Traditional Approaches Are Reactive

Traditional fraud prevention tools are used as follows. Fraud occurs. Eventually a fraud analyst discovers it. To prevent future incidents from the same fraudster, the fraud analyst attempts to block the fraudster based on a predictable characteristic, such as those shown in Figure 3-1. Most traditional fraud tools allow the fraud analyst to easily block transactions that match certain criteria. These criteria are often called business or policy rules.

As a simple example, if fraud is discovered coming from IP address 1.1.1.1, the fraud analyst then creates a business rule that prevents transactions that originate from that IP address.

There are several problems with this approach. First of all, business rules are written *after* fraudulent activity takes place and a pattern is established. When the fraud tool sees a pattern matching one defined by the business rule, it stops the activity or flags the transaction for further investigation. However, by that point a cybercriminal has already successfully defrauded an organization.

The second problem with relying on business rules to prevent fraud is that human insight alone is not enough. We simply cannot combat the sophisticated machine learning algorithms and device emulators used by fraudsters with business rules written by humans.

Finally, fraudsters change their tactics so quickly that fraud analysts can't keep up, rendering business rules obsolete. For example, a lot of organizations attempt to fight botnet fraud by identifying the botnet itself. But that's difficult to do when the botnet is constantly changing.

Silos Create Blind Spots

Remember, fraudsters use multiple techniques and target multiple points of vulnerability. If they can't get what they're after via one channel, they'll simply move to another. Traditional fraud prevention systems typically operate in silos and protect a specific business channel. A lack of integration or comprehensive visibility results in blind spots where fraudulent activity can go undetected. A next-generation fraud strategy must, therefore, be comprehensive and include multiple, integrated tools.

Fraud prevention teams also tend to work in silos, which limits their ability to stop fraud. By working independently from the security team, they miss an opportunity to stop fraud at the "front door." Teams that work together can more effectively stop some types of fraud, like account takeover and unauthorized account access.

It's common for fraud management teams to stay focused on their own organization, but that approach comes at a disadvantage. As we said earlier, cybercriminals often commit a series of fraudulent crimes within and across industries. Failing to work with others in your industry—and even other industries—to combat coordinated fraud rings results in a glaring blind spot that keeps you susceptible to this activity.

Finally, fraud management teams are blind to the devices customers are using to execute transactions. We'll discuss the value of device intelligence more in Chapters 4 and 5. For now, suffice it to say that failing to effectively leverage device intelligence to fight fraud puts the organization at a severe disadvantage.

It's All About the Customer (Experience)

Customers today have high expectations. They want to do everything online with minimal effort. They also expect you to protect their data, but they don't want to worry about security themselves. Any kind of customer friction is met with resistance. Using your digital services must be fast and easy. If it's not, they'll pack up and go elsewhere.

Meanwhile, there's rising demand for an omnichannel customer experience. This means a consistent experience whether the customer is interacting with your company via voice from a mobile device, using text chat on the desktop website, or in person at your physical store. Organizations must maintain sufficient fraud checks across all these channels while preserving the consistency of the customer experience.

You certainly can't lighten up on your fraud prevention strategy to keep your customers happy. That wouldn't last long, anyway. Instead, you need a different approach. This is the challenge before you: stop fraudulent transactions while attracting and retaining trustworthy users with competitive offerings and a streamlined customer experience. That necessitates a next-generation anti-fraud prevention program.

Chapter 4

Introducing Next-generation Fraud Prevention

In this chapter

- Understand the value of device intelligence in fighting next-generation fraud
- Learn why machine intelligence and human insight are stronger together
- Harness the power of global fraud analysts

As cybercriminals get better at defeating conventional fraud detection tools, organizations must find new, more-effective methods. Today's fraud calls for next-generation fraud prevention techniques that work with existing tools to detect fraud early on.

What the World Really Needs

Organizations need a comprehensive fraud prevention strategy that consists of the following next-generation capabilities.

Device intelligence

Every digital transaction—fraudulent or not—originates from a computing device. And each device provides a number of clues as to the user's intent. These clues come in the form of data about the device's risk and reputation. This device intelligence is key to detecting and preventing next-generation fraud.

Imagine being able to instantly evaluate any device that connects to your business. You can know if the device has been used to commit fraud in the past or if it appears to be stolen—it's jailbroken or rooted. With this knowledge, you can block the transaction in real time, before you put your business at risk.

The key to leveraging device intelligence for fraud prevention is to do so independent of personally identifiable information (PII). Keeping personal information separate helps ensure that you're meeting privacy standards. In addition, by recognizing Internet-connected devices without requiring PII, you have an independent layer of fraud prevention that's separate from identity or account data that may have been compromised.

We'll discuss device intelligence in greater depth in Chapter 5, Exploring Device Intelligence.

Comprehensive human insight + machine learning

Separately, machine learning and human insight from fraud prevention analysts can be valuable additions to your fraud prevention program. However, one without the other introduces holes in your coverage. As much as they try, fraud prevention analysts will never be able to catch up with cybercriminals. And without human insight, machine learning algorithms will always miss dangerous outliers.

But when you fight fraud with a complementary blend of human insight and machine learning, you can optimize the effectiveness of both. Machine learning can analyze millions of device and transaction attribute patterns from billions of online transactions. That technology is made even more powerful when paired with the human insight your fraud analysts possess. By "training" machine learning algorithms, you can more accurately predict the outcome of any online transaction, even if you've never before seen a particular customer or device.

We'll explore these topics in more detail in Chapter 6, Human Insight and Machine Learning.

Connecting sets of (apparently) unconnected devices

The ability to connect the dots between seemingly unrelated devices is also a critical component of a next-generation fraud prevention program. This added layer of visibility can expose hidden relationships to help teams quickly uncover fraud rings and fraud from botnets.

By revealing hidden connections between devices and accounts, you can detect instances of fraud that you may not otherwise recognize. For example, you can see if many devices have been used to access a single account, or if a new device is linked to other devices or accounts that are associated with fraud.

A team approach

Next-generation fraud prevention requires a team approach. We don't just mean that the people in your organization must work better together. That's certainly important, but what we're talking about here is the need to combine forces with the thousands of fraud professionals across every industry, around the world.

Fraudsters move from business to business, industry to industry. No organization or institution is beyond their reach. The cybercriminal who's applying for a line of credit from your organization in the United States could've been flagged just minutes prior by a financial institution on the other side of the globe. But there is strength in numbers. By working together, fraud analysts empower one another to more effectively fight fraud.

The most effective way for fraud analysts to work together is to share device reputation information. Collaborating with industry peers and those in other industries who are united against fraud unlocks the power of this data. Participating organizations benefit from tens of thousands of additional resources, tools, and experiences, without adding to their initial fraud detection investment. Every fraud analyst involved is intrinsically motivated to maintain the highest quality of evidence placement to stop repeat offenders and gain valuable, actionable insights.

A guard at the front door

It does no good to stop obvious fraudulent transactions if cybercriminals can masquerade as legitimate users to gain unauthorized access to customer accounts or your services. To prevent account takeover (ATO), a next-generation fraud prevention program requires a "guard at the front door" in the form of device-based authentication.

User devices change over time. By understanding the difference between normal changes and those that indicate risk and leveraging that information to link customers' devices to their accounts, you can create an invisible layer of defense against ATO. It works alongside your existing authentication technologies so that the device becomes a seamless second factor. By delivering a user-friendly, single-factor login experience with the security of two-factor authentication, you greatly reduce the risk of ATO and everyone is happy.

A multi-channel approach

A multi-channel approach to fraud prevention helps uncover the blind spots we discussed in Chapter 3. Every channel that customers use to interact with your business requires protection, because each is a conduit for fraud. These channels include digital properties such as the desktop website, mobile website, and mobile apps, as well as traditional ones like your call center and physical storefronts. In addition, you must be able to stop multiple types of fraud at multiple points in the customer journey: application submission, account creation, login, payments, etc.

Layering device intelligence along with other fraud prevention tools and methods across channels and the customer journey helps ensure that if one mechanism fails to catch fraudulent activity, another will. Because of its high level of effectiveness and affordable price, device intelligence should be your first layer of defense.

Chapter 5

Exploring Device Intelligence

In this chapter

- Understand the difference between device recognition and device reputation
- Learn the value of sharing device intelligence with a peer consortium
- Examine how device intelligence can enable you to shut down fraud rings

Device intelligence plays a starring role in a next-generation fraud prevention program. It helps identify fraudsters at the source, enabling you to shut down repeat offenders as well as first-time visitors with a history of fraudulent behavior.

Device intelligence provides unique insight into account creation and relationships, and exposes fraud that is invisible to other tools. Working in concert with other preventative techniques, device intelligence provides a multi-layered defense that reduces the rate and impact of online fraud.

In this chapter, we take a closer look at the different attributes of device intelligence that make it a powerful weapon against fraud.

Accurate Device Recognition

All Internet transactions have something in common: they originate from a web-enabled computing device, be it a desktop computer, laptop, tablet, mobile phone, smart watch, or even a gaming console. Every one of these devices has hundreds of attributes that, when looked at in aggregate, can form a unique identifying fingerprint. This fingerprint is a more reliable way to identify repeat visitors to your digital properties than personally identifiable information (PII), which is easily altered and abused. Thus, *device recognition* seeks to identify the device being used to conduct an online transaction. As a first line of defense against online fraud, device recognition can be a powerful tool to identify high-risk patterns of behavior.

According to research by Stone Temple, more web traffic originates from mobile devices than from desktop computers. Furthermore, the lead mobile traffic has over desktop traffic is only expected to grow. People are moving around more, and they're taking their mobile devices with them—oftentimes more than one. Our tendency to conduct Internet transactions on the go makes IP-based fraud solutions more vulnerable to false positives as well as fraud misses.

Next-generation device recognition looks at more than a device's IP address. It takes into account hundreds of unique attributes to identify a device, such as the type and version of OS running on it, and the number of applications downloaded to it.

It's important to note that device recognition must be kept separate from personal identity. If it isn't, and the identity is corrupt or inaccurate, then the device recognition data is compromised and can't be trusted.

Device Risk and Behavior

The device itself—how it's running, what it's running, and where it's running—can say a lot about the intent of the person behind it. Fraudsters attempt to hide who and where they are by altering their device properties between transactions. Legitimate customers, on the other hand, are less likely to manipulate their device data to avoid identification.

The following behaviors can indicate that the user has malicious intent:

- ☑ Using evasion techniques. Tor networks, VPNs, and anonymous proxy servers are designed to enable users to communicate on the Internet anonymously. These tools can help conceal the user's location, making it difficult to trace Internet activity.
- ☑ Demonstrating device anomalies. Incongruent or unusual details like location mismatches, time zone and IP address changes, too many devices per account, and exceeded transaction velocity thresholds can all point to a device that is being used by a fraud ring instead of a legitimate user.
- ☑ Performing a transaction from a high-risk location, IP address, or ISP where fraud frequently occurs. Users who behave in this manner may be more likely to commit fraud.
- ☑ Using jailbroken or rooted devices. If its operating system is compromised by being jailbroken or rooted, a device is at an extreme risk for being infected with malware, such as a botnet, or for being operated by a person who is using device-altering software to mask their true identity.
- ☑ Using a virtual machine or mobile emulator. Legitimate users rarely use a virtual machine or mobile emulator. Fraudsters on the other hand, use them to automate fraud attacks and to quickly switch between different (virtual) devices to fool standard fraud prevention measures.

All of these behaviors increase the risk that the user is attempting to defraud your organization. Device intelligence takes these attributes into account to create a risk profile. The organization can then set business rules regarding devices that meet pre-determined thresholds. Perhaps you decide to block them outright or flag them for further investigation.

Shattering the Myth that Mobile Devices Are Safer than Computers

There's a perception that committing fraud is more difficult from a mobile device because of operating system restrictions, biometric sensors, built-in hardware device IDs, and difficulty in automating tasks. But, fraudsters have workarounds for all of these. It's easy to jailbreak or root a mobile operating system to allow installation of special programs that help automate tasks, bypass biometric sensors, spoof geolocations, or circumvent other operating system security measures. In addition, fraudsters can run mobile phone emulators on computers, which makes them appear to be mobile devices, but with all the automation flexibility of a computer. This means it's imperative for mobile apps to include the same fraud prevention measures as their web app counterparts.

Device Reputation

It's important to know if your organization has previously flagged a device for fraudulent activity. That's a no-brainer, right? You don't knowingly let the same bad guy in twice. But imagine the impact you could have if you knew whether a device visiting your site for the first time had been flagged for fraud by *another* organization. That's what *device reputation* is all about.

Device reputation looks at the history of the device. It answers the questions: What has this device been up to? Has it been involved with any fraudulent activity? If so, what specific type of fraudulent activity, such as chargebacks, identity theft, online scams, account takeovers, cheating, and phishing?

Device reputation is a game changer. It tilts the playing field in your favor by giving you visibility beyond the here and now. If you know that a device has a history of fraudulent activity in another sector or industry, you can react differently to that device when it's introduced to your environment and reduce your risk of becoming another one of its victims.

Device reputation is most effective at preventing fraud when fraud professionals work together as part of a peer consortium that enables them to share global fraud intelligence via a

knowledge base. Fraud professionals can use this data to make real-time decisions based on the activities–both within their own industry and across others—which pose the greatest risk to them.

Device Associations

Now, let's take the notion of device reputation a step further. Imagine having the ability to uncover hidden connections between devices and accounts. In other words, imagine being able to determine the nature of the relationship between accounts and devices.

These relationships, if they can be mapped across industries and tracked globally, can be invaluable in fighting fraud. If you can determine when multiple devices are used to access a single account or even a group of accounts, then you can identify bad actors working in collusion. You have the opportunity to shut down entire fraud rings all at once.

Device associations become more powerful when the data is shared across a consortium. Not only do you understand the relationships between accounts and devices on your own digital properties, but you add the experiences and associations of other organizations around the world. Sharing this data across a large, centralized network exposes extended device-to-account relationships across multiple networks and industries. Fraud professionals everywhere help to piece together the bigger picture and put a stop to complex fraud rings that hurt everyone.

Putting It All Together

Everything we just talked about—device recognition, device risk and behavioral analysis, reputation, and association data—comprise device intelligence. As part of a next-generation fraud prevention strategy, device intelligence can empower your organization to beat today's fraudsters.

Device intelligence technology can be integrated into your native mobile and web applications. It can also be integrated into any customer touchpoint where fraud risk is a concern, such as account creation or modification, purchase, or transfer of funds.

Consumer Electronics Retailer Catches Fraud Ring—and More

Business success often brings both the good and the bad. Such was the case for a consumer electronics retailer that grew from a single storefront to a successful mail order business, and finally an online business. But while three million consumers rely on the retailer for their equipment needs, fraudsters were also targeting the business.

The retailer's commitment to customer service, fast fulfillment, and top-tier mail order service attracted reshipping scams from around the world. In one case, a "customer" placed 11 separate orders for merchandise worth tens of thousands of dollars. Even though the shipping address checked out and the credit card being used hadn't been reported stolen, the retailer was suspicious about the orders.

The consumer electronics retailer decided to investigate the orders using a device intelligence solution. With the help of iovation, the retailer discovered that even though the orders appeared to be originating from the United States based on the IP address reported, the real IP address was located in Russia. In fact, this wasn't a legitimate customer at all—it was a Russian fraud ring using stolen credit cards. Fraudsters ordered merchandise to be shipped to an associate in the States, who then reshipped the items to Russia.

In addition to identifying the Russian fraud ring, iovation also helped the retailer reduce the time it took to run fraud checks, thereby improving its customer experience by shortening the order fulfillment process.

Chapter 6

Leveraging Human Insight and Machine Learning

In this chapter

- Understand how machine learning algorithms work
- Explore the benefits of machine learning for fraud prevention
- Learn why human insight and machine learning are better together

Your people are your most important asset. They understand the business better than any technology ever will. Fraud analysts can catch certain types of fraud and react quickly to emerging patterns. But at the end of the day, your people are still people. They may miss trends that are too subtle for humans to pick up on or are only noticeable on a global scale. And at some point, they have to go home.

Fortunately, there is technology to help you out. Machine learning algorithms can analyze billions of combinations of inputs. They can detect subtle fraud trends across multiple businesses and industries more quickly and accurately than a human. And they never have to go home.

As good as they are apart, human insight and machine learning are even better together. In fact, they complement each other. In this chapter, we'll explain how human insight and machine learning can empower your organization to work smarter and more effectively in the fight against next-generation fraud.

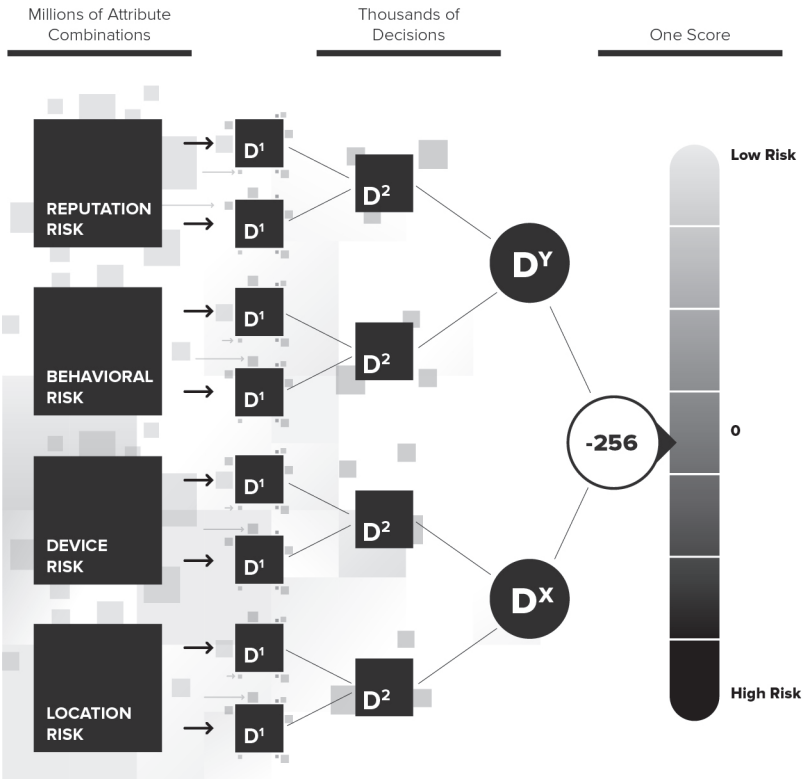


Figure 6-1: Machine learning algorithms analyze millions of device and transaction attributes searching for subtle data patterns that are used to compute fraud risk scores.

Understanding Machine Learning

Machine learning is a type of artificial intelligence that enables computers to learn without being explicitly programmed. Using statistical techniques, machine learning algorithms analyze millions of combinations of inputs to uncover unique and subtle patterns in data. In the case of device intelligence, those inputs are data pertaining to the online transaction, including the device used in the transaction, as shown in Figure 6-1.

Every online transaction has hundreds of attributes associated with it, including multiple location-related attributes, device characteristics—including anomalies—and behavioral risks,

like transaction velocities. While a fraud analyst may be able to look for patterns in one or two attributes (like an IP address and device type), machine learning can analyze millions of combinations of these attributes to determine the specific patterns that can predict risk.

For example, the pattern may be a mobile device with a specific version of Android OS, with a specific version of the browser, with a specific set of fonts and apps installed, with a transaction velocity of 30 per hour, originating from Los Angeles.

Machine learning technology constantly learns. Therefore, the patterns that are useful in predicting risk today may be different from the patterns used next week. In this way, your fraud prevention ability is constantly improving itself without any human intervention.

Two key components are needed to build a machine learning model. The first is a huge dataset, which is required because of the statistical nature of machine learning. We're talking billions of data points. The second requirement is a way to train the model. Models need to understand what's considered good and what's considered bad. With device intelligence, we have a perfect means for this training: device reputation. By analyzing the attributes of devices and transactions that have been flagged as fraudulent (reputation), machine learning can be trained and then predict when new transactions will be fraudulent.

Not all machine learning models are the same. The best model for fraud prevention has the following characteristics:

- ☑ It uses a systematic means for training, such as device reputation.
- ☑ It looks at global datasets, rather than that of an individual business.
- ☑ It's ready for use on Day 1.

Be cautious of machine learning models that require months of training before they are able to produce useful results.

Why you need it

We're not exaggerating when we say that machine learning can transform your fraud prevention program. It can optimize your processes and improve your effectiveness, all while reducing your costs.

Consider your review queues. Machine learning can reduce the cost of manual reviews by predicting the trustworthiness or riskiness of a transaction. By knowing which transactions pose the greatest risk, you can focus your efforts on those first. In the meantime, you can fast-track good transactions and reserve more expensive verification methods for situations when they're absolutely necessary.

Machine learning can also help reduce fraud losses. By analyzing every transaction, machine learning can predict which transactions will go bad, even if your own manual fraud rules do not. Machine learning can also stop fraud attempts that have been seen elsewhere by leveraging global fraud and risk insights from other businesses.

Finally, by identifying good customers, machine learning enables you to improve the customer experience. You can grow revenue faster by offering special incentives to new customers and high-value incentives to existing customers. You can also increase customer satisfaction by eliminating lengthy fraud reviews and delays.

Maximizing Human Insight

The real value of machine learning is realized when it's paired with human insight. Fraud analysts understand your business and its unique risks, and the industry at large. They can apply this knowledge to give proper context and nuance to the machine learning data.

Human insight is great for stopping targeted threats and implementing business policy. For example, you know that if an online transaction involves a device with a reputation for being fraudulent, the chances are very high that any future transactions from that device will also be fraudulent. Therefore, your fraud analysts create a business/policy rule that prohibits transactions from devices with a bad reputation—effectively stopping the threat.

Chapter 7

Harnessing The Power of Next-generation Device Intelligence

In this chapter

- Learn how device intelligence enables you to uncover more fraud
- Explore the capabilities that allow you to improve operational efficiencies
- Understand how device intelligence delivers value beyond the fraud prevention organization

When deployed as part of a comprehensive fraud prevention program, next-generation device intelligence helps organizations fight fraud more effectively and efficiently. It can also help transform the fraud prevention organization from a cost center to a revenue generator. In this chapter, we explore how advanced device intelligence delivers these benefits and more.

Catch More Fraud

Device intelligence gives organizations the visibility they need to find more fraud. With greater transparency from device intelligence, fraudsters can no longer hide behind their devices and engage in criminal activity with a high degree of anonymity. Nor can they simply alter a synthetic identity to establish a seemingly legitimate account.

Device intelligence detects patterns on devices used to commit fraud. It shines a light on cybercriminals and exposes them for

who they actually are. As a result, organizations can uncover fraud that isn't detected by identity-based solutions alone.

Device intelligence also enables organizations to find relationships between seemingly unrelated incidents of fraud. By identifying fraudsters who are working in collusion or using multiple devices from anywhere in the world, organizations can efficiently shut down entire fraud rings all at once. How's that for a day's work?

The value of device intelligence doesn't just come from catching *more* fraud. It also comes from catching more fraud at the *right time*. By blocking fraudulent transactions early in a business transaction, organizations can eliminate costly detection tools and procedures from the fraud detection process. For example, device intelligence can reduce the average cost of approving/disapproving a credit card application by identifying fraudulent submissions at the gateway.

Increase Operational Efficiency

It's common sense. When you automate the process of catching more fraud, as device intelligence allows you to do, your operational efficiency improves. Stopping fraud upstream reduces the number of suspicious transactions that are queued for manual review. Organizations can potentially reallocate resources and reduce the need for additional headcount.

Device intelligence, when used with machine learning and human insight, provides more accurate analysis of every single digital transaction in real time. Even new customers and/or devices are analyzed, keeping them out of your review queue.

Device intelligence also exhibits fewer false positives than other fraud prevention methods. This means smaller review queues. By reducing time spent analyzing, evaluating, diagnosing, and closing potentially good and bad transactions, fraud prevention organizations can increase the efficiency of their fraud detection process—and even turn it into a revenue generator. Your fraud analysts are happier—and customers are, too. Streamlining the decision process allows organizations to accept good business faster, eliminate processing delays, and improve overall customer satisfaction.

Ensure Compliance

Device intelligence can also help you comply with regulatory standards, such as the European Union's revised Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR), and the terms and conditions of licensing agreements. For example, by identifying the devices used to set up new accounts, organizations can stop servicing customers from countries they're not licensed to serve.

A device intelligence solution can also address U.S. Federal Financial Institutions Examination Council (FFIEC) requirements by ensuring that transactions are assessed and scored for risk, and by meeting complex device identification requirements.

Beyond Fraud Prevention

Let's face it: it's not always easy for the fraud prevention organization to get the budget it needs to carry out its responsibilities. Device intelligence can change that dynamic, too. The benefits it offers can extend beyond your organization to help others achieve their business goals.

Account access and security

When used by the IT security organization, device intelligence can help shore up protections for secure account access. Stealing user credentials is a highly effective and popular method for cybercriminals to gain access to private networks. These stolen credentials look legitimate to IT systems, so they grant the unauthorized user access to all the systems and data to which the legitimate user is entitled. Privileged accounts, like those belonging to executives or IT professionals, permit access to more systems and sensitive data than regular user accounts, so they pose an even greater risk.

A device intelligence solution doesn't care what credentials a user submits. It's all about the device. Regardless of the username and password submitted, device intelligence will look at that device to determine if it has a history associated with fraud, looks suspicious in the here and now, or has exhibited behavior that indicates a high risk of fraudulent activity. IT

can then block these access attempts with a high degree of confidence that they're not preventing the CEO from logging in with a new device.

User experience

Customer service and the user experience have become so important in the Mobile Age that every organization keeps the customer on its radar. Device intelligence helps improve the user experience even while catching more fraudsters. The process of identifying and analyzing each device takes microseconds. The user experience doesn't suffer at all. In fact, it's improved because fewer false positives mean you're less likely to upset a good customer by blocking or delaying their transaction.

It only takes one fraudulent incident to discourage a customer from returning to your business. With data breaches and identity theft making mainstream news, customers want to know what businesses are doing to protect their accounts and information. Educating customers on your use of device intelligence can help earn and maintain their trust.

Business partners can also benefit from device intelligence. The information gleaned from a device can be passed on to these entities to help them make better-informed decisions about referred customers.

From Cost Center to Profit Center

The fraud prevention organization in a company is typically considered a cost center. A device intelligence solution can change that. Consider all the things you can do to generate revenues when you use device intelligence to confidently identify new and repeat customers who do not pose a fraud risk:

- Fast track them through specific business transactions
- Offer promotions to new customers when they register online
- Present upselling and cross-selling offers to existing customers when they log in
- Pre-qualify customers for new loans, discounts, etc.
- Present offers from business partners
- Empower live agents by providing them with device intelligence data on good customers
- Drive incremental revenue by using device intelligence to develop new digital services and functionality based on customer accounts and activity across business lines
- Offer new, high-risk services that increase customer convenience, such as remote deposit capture, which lets customers photograph or scan a check for immediate deposit into their accounts

Bank Puts an End to Impersonation-based Fraud

A consumer finance bank founded on the principles of value and simplicity was attracting more than customers. Fraudsters had taken notice of the firm, making it important for the bank's fraud department to identify potential scams before approving and fulfilling loan applications.

Social engineering is often associated with dating sites. Fraudsters use the technique to trick victims into divulging personal information. In the case of the financial institution, fraudsters were using these details to take out loans in the victim's name. The bank wanted to reduce its fraud losses from impersonation without impacting the user experience of its good customers.

The financial institution implemented iovation's online fraud prevention and detection solution. By using this solution to identify every device visiting its loan application page, the bank was able to assess each device's reputation and association with other devices. The bank learned if a device had a history of fraud itself, or was associated with other devices with a history of fraud. Within six months of implementation, iovation stopped almost every instance of impersonation-based fraud at the bank, yielding an 850% return on investment during that timeframe.

Chapter 8

10 Buying Criteria for Next-gen Fraud Prevention

In this chapter

- Learn what questions to ask fraud prevention solution providers
- Explore the capabilities that will help you catch advanced fraud—today and tomorrow

A next-generation fraud prevention solution based on device intelligence addresses the problems that currently plague online businesses and is necessary for doing business in the Mobile Age. As more of your business moves online, and your customers move with it, you'll need increasingly robust fraud prevention services.

In this chapter, we provide 10 criteria for choosing an online fraud prevention platform that will take you and your users safely into the future. You need a solution that addresses all of them to achieve true protection.

Advanced Device Recognition

Don't be fooled into thinking that device recognition is as simple as storing a cookie in a browser's cache. Solutions vary in their ability to recognize devices, and you need to dive deep into their technology. Ask vendors if they use a multi-layered approach to device recognition. If they primarily rely on one technique (such as cookie placement), then it will be easy for fraudsters to circumvent recognition. Other key capabilities to look for include:

- ☑ Recognizing a device without directly identifiable personal information (such as email or phone number)
- ☑ Recognizing the same device across businesses and industries, again without requiring personal information
- ☑ Recognizing any type of online device (including smartphones, smart watches, gaming consoles, and IoT devices) that can connect to the Internet

Machine Learning

A comprehensive fraud prevention solution must include machine learning capability, especially for catching emergent fraud. However, it's important to understand how this capability is used and what it does. First, find out what methodology each vendor used to develop their model. Ask what data attributes (for example: transaction attributes, device attributes, and behavior attributes) are used by the model. Query vendors about how they train their model and, in particular, how they train it to recognize fraudulent transactions. Ask how often they update/retrain the model, and if they use only their own data or data from all vendors. Neither one is necessarily better than the other, but they do catch different things. Also, determine how the machine learning results are returned for the transaction—as a risk score, or something else? See if the results are returned in real time.

Human Insight

Just as machine learning is important for spotting subtle fraudulent patterns and emerging new fraud trends, being able to easily define manual fraud and policy rules continues to be critical for fraud prevention. Most businesses have hundreds of different manual policy rules. Ask the vendor to demonstrate how easy it is to change or add a business/policy rule using their solution. Ask to see a list of all device and transaction attributes that can be used in business rules. Ensure that the business/policy capabilities of the tool are easily combined with the vendor's machine learning offering.

Online & Mobile Support

A device intelligence solution must support both web and mobile apps. Look for a solution that is JavaScript based and has native software development kits (SDKs) for common mobile operating systems.

Granular Device Reputation

Ask each vendor if their device intelligence solution provides device reputation capabilities and how detailed the reputation is. For example, find out if you can distinguish between a device with a reputation of stolen credit usage and another with a reputation of cheating in gambling.

Reputation is different from a risk assessment based on device characteristics or behavior. Device reputation is established when a fraud professional tags a device with a reputation report after fraud or abuse is confirmed. A risk assessment is a numeric computation based on the riskiness of certain device attributes and doesn't explain ***why*** a device is risky.

Active Industry Participation

Because device reputation is based on human insight, it's a good idea to ask vendors how many of their customers actively participate by providing feedback. Ask which industries those customers represent and how many reputation reports they've filed. Also find out if the network is global or regional.

Device Associations

Fraud rings are comprised of multiple people and multiple devices. Therefore, a device intelligence solution should be able to report associations between devices. If a fraud ring targets your business with one device and then returns with different devices, you need to know that they are connected. In addition, association reports can help identify a device as having been associated with prior fraud, even if a fraudster attempts to pass it off as new by wiping it clean.

Comprehensive Device Risks

Because device intelligence looks at risk attributes of the device, the types of risk checks offered by the solution should be comprehensive. Device type, device attributes, operating system attributes, and browser attributes should be available for assessing risk. In addition, multiple geolocation attributes should be available so they can be cross-checked. Geolocation attributes such as IP address, ISP location, cell tower location, and various browser and device location settings help establish if the device is actually where it reports to be. Rooted or jailbroken detection should be available as well.

Fraudsters are constantly changing techniques, so generation of a risk assessment score by machine learning or other advanced algorithms is highly desirable.

Flexible Configuration

To reduce your total cost of ownership, select a device intelligence solution that is provided as a service. Ensure that it offers a robust and modern API framework such as REST.

Most importantly, be sure that you can vary protection for all of your customer interaction points. For example, stopping fraud at new account creation (or loan application) is much different than stopping account takeover or payment fraud. You should be able to vary the device risks for each interaction point.

Ask vendors about their onboarding process. Stopping fraud can be complex. You should have the full support of the vendor's fraud prevention and solution experts not only during onboarding, but after the solution is in place.

Service Reliability

When procuring a solution that is supplied as Software-as-a-Service, look for an uptime reliability of 99.99% or higher. Since this is a real-time service, API calls must happen in real time. Calls that take longer than 150 ms will likely impact the user experience.

Glossary

account takeover (ATO): A type of third-party fraud in which the fraudster takes over someone else's account by pretending to be that person or by using stolen credentials.

botnet: An interconnected network of computers that are infected with malware without the user's knowledge. Botnets are used by cybercriminals to spread spam, conduct distributed denial-of-service attacks, and steal personally identifiable information (PII) to commit financial fraud.

distributed denial-of-service (DDOS): An Internet-based attack that aims to compromise systems or disrupt network services by flooding the bandwidth of a targeted system.

device associations: The ability to create connections between devices without need of PII. If one device has been confirmed to be fraudulent, then the risk of associated devices being fraudulent is higher as well.

device recognition: The identification of a device based on its unique attributes at the present moment.

device reputation: A device's past history of confirmed fraud or abuse, which can be an indicator of whether it poses a risk at the present time. Device reputation is usually determined by a fraud analyst after confirming that fraud or abuse has occurred.

emulators and virtual machines: These are software programs that run on a computer and emulate a different type of device altogether. For example, an iPhone emulator may run on a Windows PC and transactions originating from it may appear to be coming from an iPhone. Fraudsters use these to create large inventory of "virtual" devices as well as to automate keystroke entry.

evasion: Fraudsters often try to trick fraud prevention solutions by masking their true identity or location. This is known as evasion or evasive techniques. The most common type is using an IP proxy such as Tor.

first-party fraud: A type of fraud committed by an individual using their own name and account information.

jailbreak or rooted: An activity by which a user intentionally disables safeguards in the operating system, often for the purposes of installing unsafe software applications.

machine learning: A type of artificial intelligence that enables computers to learn without being explicitly programmed.

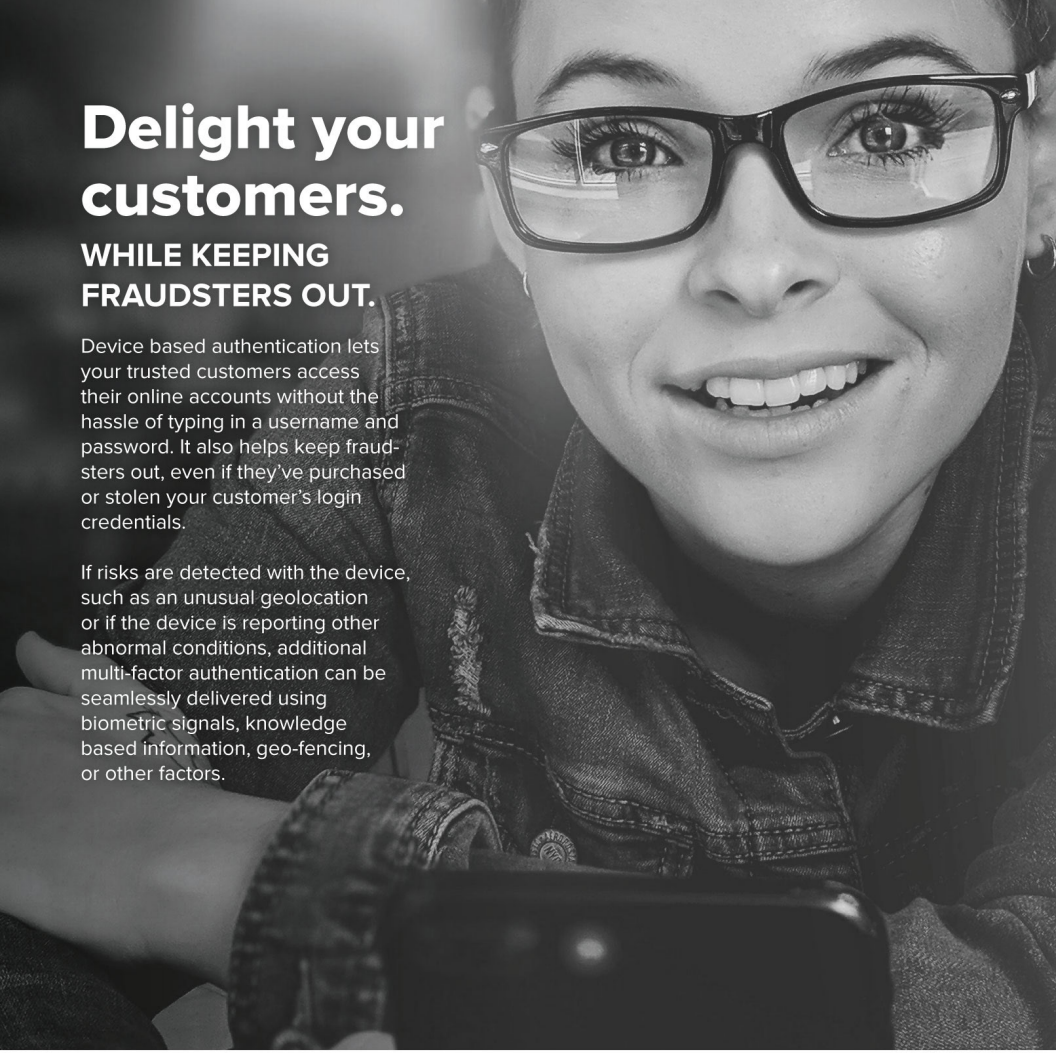
personally identifiable information (PII): Information such as name, phone number, and mailing address that can be used on its own or with other information to identify, contact, or locate an individual.

social engineering: A non-technical attack that involves manipulating people in an effort to get them to disclose sensitive information or do something they wouldn't normally do, such as go against corporate policy.

synthetic identity: A fake identity created by combining various pieces of personal and financial data belonging to different people. These new identities look legitimate to companies.

The Onion Router (Tor): A proxy-masking service that anonymizes IP addresses, making it difficult to determine where a device is really located.

third-party fraud: A type of fraud that occurs when an individual or group, such as a fraud ring, commits fraud under someone else's identity.



Delight your customers.

WHILE KEEPING FRAUDSTERS OUT.

Device based authentication lets your trusted customers access their online accounts without the hassle of typing in a username and password. It also helps keep fraudsters out, even if they've purchased or stolen your customer's login credentials.

If risks are detected with the device, such as an unusual geolocation or if the device is reporting other abnormal conditions, additional multi-factor authentication can be seamlessly delivered using biometric signals, knowledge based information, geo-fencing, or other factors.

NEXT GEN FRAUD PREVENTION AND ADAPTIVE AUTHENTICATION GO HAND IN HAND.

iovation's authentication suite and fraud prevention suite work together to provide you the next gen framework for fighting fraud.

ClearKey

Reduce friction for customers by providing an invisible, hassle-free web experience utilizing device recognition.

LaunchKey

Leverage adaptable, risk- based multifactor authentication to secure online accounts.

FraudForce

Stop fraud in real time with device recognition technology and a global network with over 40M confirmed fraud cases.

SureScore

Predict if a transaction can be trusted or will become fraudulent using machine learning and analytics.

To learn more, visit: **www.iovation.com**

iovation®
A TransUnion® Company

It's time to evolve your fraud prevention strategy. Learn how to reduce losses and catch more fraud cost-effectively with next-generation fraud prevention.

Welcome to the Mobile Age, where cybercriminals have abundant opportunities to commit fraud, and fraud prevention organizations are challenged with stopping them—without impacting the user experience for good customers. This book describes how to use next-generation fraud prevention techniques to prevent fraud early in a transaction to reduce costs, prevent losses, and improve the user experience.

- Introducing fraud in the mobile age — learn how the ability to exchange data quickly while on the go enables fraud
- Understanding the enemy — explore the different types of fraud, and the various tools and techniques cybercriminals use to commit fraud
- Exploring device intelligence — examine how device intelligence can enable you to shut down fraud rings
- Leveraging human insight and machine learning — see how human insight and machine learning should work together in the fight against fraud
- Harnessing the power of next-generation device intelligence — learn the benefits of leveraging device intelligence beyond stopping fraud
- Selecting the solution — know exactly what to look for, and what to avoid, when evaluating next-generation fraud prevention solutions

About the Authors

A former editor of SearchSecurity.com, Crystal Bedell is a senior marketing consultant specializing in cybersecurity. She's been helping technology providers create engaging content since 2000. Eddie Glenn is a senior product marketing manager at iovation. Eddie has over 25 years of experience in developing and managing critical software systems.

CYBEREDGE PRESS

Not for resale

ISBN 978-0-9903354-4-3