"Use a layered approach to detect online fraud in order to increase your chances of beating the fraudsters"

Gartner, Market Guide for Online Fraud Detection, 2 June 2014.

"Give priority to vendors that provide multiple layers of protection, users and/or account profiling and behavioral analytics"

Gartner, Market Guide for Online Fraud Detection, 2 June 2014.

From the Gartner Files:

Market Guide for Online Fraud Detection

The online fraud detection market has substantially transformed in the past two years, trying to keep pace with rapid advances and expansions in cybercrime. This Market Guide will help fraud managers navigate this amorphous space so they can make "rightsize" fraud detection purchasing decisions.

Key Findings

- The Web fraud detection market has transformed into the broader online fraud detection (OFD) market, which absorbs fraud detection for Web, mobile and telephony-based (that is, call center and voice response unit [VRU]) commerce.
- Identity-proofing functions are integrating with OFD technology, reflecting the need to continually assess the risk of individuals using internal and external identity information.
- The OFD market is characterized by multiple point solutions and innovative niche vendors, along with vendors trying to provide "one-stop shop" fraud detection services.
- One-stop fraud detection solutions don't always have the most advanced "weaponry" on the market for combating advanced attacks.

Recommendations

Fraud managers:

- Use a layered approach to detect online fraud in order to increase your chances of beating the fraudsters. Incorporate endpoint-centric (Layer 1), navigation-centric (Layer 2) and user/account-centric (Layer 3) fraud detection functionality.
- Give priority to vendors that provide multiple layers of protection, user and/or account profiling, and behavioral analytics.
- Give extra weighting and consideration to vendors that bring actionable external identity or threat intelligence to the OFD application, once you have the initial fraud detection layers implemented.
- Use a best-of-breed approach to combat advanced cyberattacks, if you have the resources to integrate different products and services into a common alert management system that correlates and prioritizes fraud events.

Strategic Planning Assumption

By 2017, passive biometric analysis will become a standard feature of at least 30% of one-stop fraud detection solutions — up from less than 1% today.

Market Definition

This document was revised on 7 July 2014. The document you are viewing is the corrected version.

The OFD market is composed of vendors that provide products or services that help an organization detect fraud that occurs over the Web, mobile or other telephony-based channels (that is, call center and VRU) by:

- Running background processes (that users cannot see or detect) that use up to hundreds of attributes — such as geolocation, device characteristics, user behavior, navigation and transaction activity — to determine the likelihood of fraudulent users or transactions
- Comparing this information to expected behavior using machine learning or statistical algorithms, or rules that define "abnormal" behavior and activities (see Note 1)

OFD vendors detect online fraud as transactions occur, one at a time. They provide solutions for the Web, mobile or telephony channels from one or more of the first three layers of Gartner's five-layer fraud prevention — that is, endpoint-centric (Layer 1), navigation-centric (Layer 2) and user- or account-centric for a specific channel (Layer 3; see Note 2 for a description of the five layers of fraud prevention).

OFD systems typically return alerts and results (such as scores with supporting data) to enterprise users that enable the enterprise to take appropriate follow-up action, such as:

- Suspending the transaction if actual behavior is out of range with what's expected
- Conducting further review and investigation of the transaction, as warranted
- Triggering automated user authentication and transaction verification functions that interact with the user in order to determine the legitimacy of the user or transaction

OFD applies mainly to three use cases:

- Detecting account takeover, which can occur when user account credentials are stolen or authenticated sessions are hijacked (for example, via malware-based attacks)
- Detecting new account fraud (for example, when a fraudster sets up a new account using a stolen or fictitious identity)
- Detecting the use of a stolen financial account (for example, a stolen credit card) by a fraudster when he or she makes a purchase

Market Direction

This OFD Market Guide replaces Gartner's "Magic Quadrant for Web Fraud Detection," reflecting the fragmentation, consolidation and expansion of the OFD market. These market dynamics were witnessed during several mergers and acquisitions in 2012 and 2013, while, at the same time, many new entrants emerged from different corners of the market.

For example, in 2012, RSA, The Security Division of EMC, acquired Silver Tail Systems and Diebold acquired Gas Tecnologia. In 2013, Experian acquired 41st Parameter, F5 acquired Versafe, IBM acquired Trusteer and NCR bought Alaric Systems. (All acquisition targets except Versafe — a relative newcomer — were covered in Gartner's Web Fraud Detection Magic Quadrants.)

At the same time as the market was consolidating, user requirements in an increasingly complex online world under cyberattack have driven innovation in separate (but related) fraud detection capabilities, which are needed to stay ahead of evolving criminal methods.1 Over time, these disparate capabilities and the vendors that support them will come together in a consolidated market that enables integrated solutions. The OFD market will further consolidate by 2016 as larger vendors in the call center, identity proofing, and banking and e-commerce fraud detection businesses acquire one-third of the niche or smaller startup players of 2014.

These separate (but related) user requirements include the need for the following functions (see more on these below in the Market Analysis section):

- One-stop fraud detection solutions
- Continuous identity proofing
- External threat intelligence
- Telephony-based channel fraud detection
- Mobile-centric fraud detection
- Smarter risk scoring models — self-adjusting and self-learning
- Passive biometric analysis

In the end, the ultimate goal of OFD is:

- Continuous behavioral profiling of users, accounts and entities across online channels.
- Enriching that profile with internal and external identity information.
- Ingesting and integrating external threat intelligence with fraud detection analysis and operations.
- Using these rich data sources (from the three preceding bullets) to compare incoming transactions across online channels to existing profiles and norms of user or entity behavior in order to detect fraud. As noted above, fraud detection uses rules, statistical models or both.

Market Analysis

Gartner separates the OFD market into three main buyer segments, based on the sectors that vendors target with their products:

"The ultimate goal of OFD is: continuous behavioral profiling of users, accounts and entities across online channels"

Gartner, Market Guide for Online Fraud Detection, 2 June 2014.

"Most organizations cannot keep up with the latest attack vectors"

Gartner, Market Guide for Online Fraud Detection, 2 June 2014.

"Prefer vendors that provide solutions covering as many of the three layers of OFD as possible"

Gartner, Market Guide for Online Fraud Detection, 2 June 2014.

"Continually monitor and analyze user behavior, as soon as a relationship with an individual begins until it ends, because the life circumstances of the individual may change, or the identity may have been bad to start with"

Gartner, Identity Proofing Revisited as Data Confidentiality Dies, Avivah Litan, 12 December 2013.

- **Banking:** This also includes payments between all parties that accept, transmit or process payments.
- **E-commerce:** This also includes e-commerce payments between online retailers or other online payment acceptors and the payment networks.
- **Sector-neutral:** This includes, for example, banking, payments, e-commerce, gaming, social networking, telecom, e-government, education, transportation and other sectors.

Within each of these segments, vendors offer various categories of fraud detection capabilities. These categories reflect the focus of particular vendors and how they approach the OFD market:

- **One-stop fraud detection solutions:** Most organizations cannot keep up with the latest attack vectors and what is needed to mitigate attack damage, and therefore prefer vendors that provide solutions covering as many of the three layers of OFD as possible. This way, users can meet most of their fraud detection needs by engaging with one supplier.
    - **One-stop fraud detection managed services:** Some enterprises want to outsource the review and management of suspect transactions. Emerging managed services guarantee payments on reviewed transactions in return for a percentage of the value. This service can be particularly useful for internally declined transactions that could benefit from additional review for potential acceptance, and also for international transactions in which companies have little experience with fraud detection.
- **Continuous identity proofing:** External identity information needs to be checked and analyzed in conjunction with user activity within the organization to help inform when an identity "goes bad" because of changes in life circumstances, or perhaps when an identity (or parts thereof, such as a device or email address) is hijacked by a fraudster.

Here, we see vendors helping to assess the risk of an identity by correlating an identity's attributes with external information based on:

- **Public records**, including personally identifiable information (PII) data from data aggregators, credit bureaus, news feeds, driver's license databases and more. PII data is regulated.
- **Non-PII data networks**, which identify entities and relationships associated with suspect or fraudulent activities using non-PII data (such as endpoint device identities, IP addresses, email addresses, phone numbers and so on). Non-PII data typically is not regulated, but there are restrictions in some countries (for example, in Europe) in associating IP addresses with people's names.
- **Public social network information** from networks (such as Facebook and LinkedIn) that assess an individual's social footprint and associated risk. Use of publicly available social network information is not regulated.

- **External threat intelligence integrated directly into OFD:** Organizations benefit from intelligence culled about cybercriminals and potential attacks, which is available in the criminal underground and shared across potential victim organizations. For example, most cyberattacks employ malware that is either targeted against a specific enterprise or has been used before to attack companies in a specific sector (for example, retail or financial services). Vendors with capabilities in malware identification and analysis, and in threat intelligence, have moved into the OFD market. They make their intelligence actionable in the fraud detection system — for example, by integrating blacklists of URLs, malware signatures or "bad" IP addresses.
- **Telephony-based channel fraud detection:** As enterprises tighten up controls across various points of entry (such as Web channels, kiosks and points of sale), fraudsters are more frequently exploiting traditionally less protected telephony channels, including call centers and VRUs. Large financial services companies report that about 30% of their fraud occurs via compromises of multiple channels that include the telephony channel, and several vendors now sell solutions to stop telephony-based fraud. This type of fraud can be automated or conducted by a human.

- Mobile-centric and multiple aspects for fraud detection: Mobile commerce has presented significant effectiveness and usability challenges to existing ways of identifying end users and their devices, which worked relatively well on desktop and laptop computers. As such, enterprises are looking for fraud detection solutions that do not inconvenience mobile users, but do ensure that applications are accessed only by legitimate, authorized users. (For example, device fingerprinting is ineffective on most mobile devices, while it considerably helps to detect fraud originating from desktops and laptops; however, it is becoming less effective at detecting access via proxy servers.) Mobile-centric fraud detection looks for signs of fraud at the device, application and user level.

- **Smarter risk scoring models — self-adjusting and self-learning:**

  - **Self-adjusting models:** These reduce the burden on users to help keep vendor risk scoring models up to date by informing the model on confirmed fraud events. Such user participation has often been difficult to maintain, so vendor models often get out of date and, therefore, are unable to recognize new fraud trends. Self-adjusting models are enabled by baselining online activity and looking for anomalies relative to the baseline, with the assumption that most online activity is "good" or legitimate.

  - **Self-learning models:** Ultimately, users want to be able to throw their data into a modeling system that can find fraud patterns they have never even considered. In other words, users want an application that can figure out which activities are suspect or fraudulent without them or the vendor having to tell the application anything. Some people refer to this as "artificial intelligence," which is starting to appear in the OFD market.

- **Passive biometric analysis:** Here, biometric analysis is done "behind the scenes" and is transparent or unknown to the user (unless an organization chooses to tell the user it is occurring). There is no user enrollment necessary. Over time, the system is trained on a user's biometric "signature" so that it can compare the signature to a fraudster's on a blacklist, or to ongoing user behavior to determine whether the legitimate user is being impersonated. The use of passive voice recognition and passive gesture dynamics — that is, behavioral techniques in which user movements on a device are tracked and measured — have already proved to be very useful in the OFD market.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Representative vendors are listed by market category, as described in the Market Analysis section above. Their categorization is based on their native technology, not on any partner solutions they have integrated or can potentially integrate. (The only exception to this is with identity-proofing vendors, whose core mission is largely based on their ability to aggregate different identity intelligence data sources.)

Below is a list of representative OFD vendors. Table 1 depicts the sectors these vendors target, and Table 2 depicts the functional capabilities of these vendors:

- Accertify
- ACI Worldwide
- Agnitio
- Ayasdi
- BAE Systems Applied Intelligence
- BioCatch
- CA Technologies (Arcot Systems)
- Contact Solutions
- CustomerXPs
- CyberSource
- Digital Resolve
- Easy Solutions
- Experian (41st Parameter)
- F5 (Versafe)
- Feedzai

"Passive biometric analysis: here biometric analysis is done "behind the scenes" and is transparent or unknown to the user"

Gartner, Market Guide for Online Fraud Detection, 2 June 2014.

- Fox-IT
- GBGroup
- Guardian Analytics
- IBM (Trusteer)
- IDology
- InAuth
- Inform
- Intellinx
- iovation
- Kaspersky Lab
- Kount
- LifeLock (ID Analytics)
- mSignia
- NCR (Alaric Systems)
- Nice Actimize
- NuData Security
- Pindrop Security
- Plus-TI
- ReD
- Riskified
- RSA, The Security Division of EMC
- SAS
- Sift Science
- Signifyd
- Socure
- ThreatMetrix
- Trustev
- Verint Systems (Victrio)

Table 1. Target Sectors

Vendor	Banking	E-Commerce	Sector-Neutral
Accertify		x	
ACI Worldwide	x		
Agnitio			x
Ayasdi			x
BAE Systems Applied Intelligence			x
BioCatch			x
CA Technologies (Arcot Systems)	x	x	
Contact Solutions			x
CustomerXPs	x		
CyberSource		x	
Digital Resolve			x
Easy Solutions			x
Experian (41st Parameter)			x
F5 (Versafe)			x
Feedzai	x		
Fox-IT	x	x	
GBGroup			x
Guardian Analytics	x		
IBM (Trusteer)	x		
IDology			x
InAuth			x
Inform	x		
Intellinx			x
iovation			x
Kaspersky Lab	x		
Kount		x	
LifeLock (ID Analytics)			x
mSignia			x
NCR (Alaric Systems)	x	x	
Nice Actimize	x		
NuData Security			x
Pindrop Security			x
Plus-TI	x		
ReD	x	x	
Riskified		x	
RSA			x
SAS			x
Sift Science			x
Signifyd			x
Socure			x
ThreatMetrix			x
Trustev			x
Verint Systems (Victrio)			x

Source: Gartner (June 2014)

Table 2. Functional Capabilities and Focus

					Identity Proofing				Telephony Channel		Passive Biometric Analysis			
	Multiple Layers (1-3)	Endpoint-Centric (Layer 1)	User/Account-Centric (Layer 3)	Mobile Platform Multiaspect	Non-PII Networks	Social Networks	Public (PII) Information	External Threat Intelligence	Call Center	Voice Response Units	Voice	Gestures	Self-Learning Models	Managed Fraud Detection Svc.
Accertify			x											x
ACI Worldwide			x											
Agnitio											x			
Ayasdi													x	
BAE Systems Applied Intelligence	x							x						
BioCatch	x											x		
CA Technologies (Arcot Systems)	x													
Contact Solutions										x				
CustomerXPs			x											
CyberSource			x											x
Digital Resolve			x					x						
Easy Solutions	x							x						
Experian (41st Parameter)	x				x									x
F5 (Versafe)		x												
Feedzai			x											
Fox-IT	x							x						
GBGroup					x		x							
Guardian Analytics			x											x
IBM (Trusteer)	x							x						
IDology							x							
InAuth		x												
Inform			x											
Intellinx			x											
iovation		x			x									
Kaspersky Lab	x							x						
Kount	x													
LifeLock (ID Analytics)					x		x							
mSignia				x										
NCR (Alaric Systems)			x											
Nice Actimize			x						x		x			
NuData Security	x				x							x	x	
Pindrop Security									x					
Plus-TI			x											
ReD			x		x									
Riskified														x
RSA	x							x					x	x
SAS			x											
Sift Science	x				x									
Signifyd						x								
Socure						x								
ThreatMetrix		x			x									
Trustev						x	x							
Verint Systems (Victrio)									x					

Source: Gartner (June 2014)

"Give priority to vendors that provide multiple layers of protection, users and/or account profiling, and behavioral analytics"

Gartner, Market Guide for Online Fraud Detection, 2 June 2014.

Market Recommendations

Fraud managers:

- Employ a layered OFD approach, and, at a minimum, use solutions that integrate endpoint-centric (Layer 1) with user- and account-centric (Layer 3) fraud detection.
- Give priority to vendors that provide multiple layers of protection, user and/or account profiling, and behavioral analytics using statistical models and rules.
- Give extra weighting and consideration to vendors that bring actionable external identity or threat intelligence to the OFD application.
    - If you already have a strong installed base of fraud detection software, then consider using just the external intelligence data from other OFD vendors to strengthen your existing fraud detection systems.
- Recognize that resolving difficult challenges and stopping advancing attacks in the online channel will require piecing together niche solutions. Most of the innovation that addresses rapidly evolving criminal techniques is introduced by small niche vendors, not the ones that offer one-stop platforms.
    - This will only be a practical option if your enterprise has considerable resources to devote to this exercise, and already has a significant installed base of fraud detection software and services.
- Integrate disparate point solutions into a common alert management system wherein alerts and their attributes can be weighted and correlated to highlight the most suspect alerts and events that need immediate attention.
    - Otherwise, you will have too many alert management systems to manage, and your organization will not benefit from correlating the different events that are alerted.
- Feed fraud data into a big data warehouse to get an enterprise view of fraud and security issues, and to support Layer 5 fraud detection.

Evidence

1 Each year, Gartner fields several hundred inquiries from clients worldwide regarding fraud detection and prevention. These calls unearth common requirements and trends across the globe in relation to combating fraud.

Note 1

Risk Scoring and Modeling

Optimally, vendors should support user and entity profiling — that is, a user or entity's ongoing behavior is captured in a profile, against which new activity can subsequently be compared to determine the likelihood that the activity is legitimate.

This anomaly detection is accomplished using statistical models, rules or a combination of both. In addition, one of each type of statistical model, as described below, should be deployed for best results. Statistical models are based on either:

- Confirmed fraud and "bad" behavior, which users need to tell the model about.
- "Normal behavior," most of which is assumed to be "good." This type of model is best when there is no history of confirmed fraud, or when fraud analysts or other enterprise users want the model to be self-maintaining. There is no need for users to tell the model what is normal; rather, it can figure this out by itself by baselining various activities and entity behaviors. Anomalies will be detected because they will stand out relative to the baseline. Not all anomalies represent fraud.

Note 2

Five Layers of Fraud Prevention

Gartner breaks down fraud prevention into five layers:

- **Layer 1** is endpoint-centric; it involves technologies deployed in the context of users and the endpoints they use. Layer 1 technologies include secure browsing applications or hardware, as well as transaction-signing devices. These devices can be dedicated tokens, telephones, PCs and more. Out-of-band or dedicated hardware-based

transaction verification affords stronger security and a higher level of assurance than in-band processes do. The technologies in this layer typically can be deployed faster than those in subsequent layers, and go a long way toward defeating malware-based attacks.

- **Layer 2** is navigation-centric; it monitors and analyzes session navigation behavior and compares it with navigation patterns that are expected on that given site, or uses rules that identify abnormal and suspect navigation patterns. It's useful for spotting individual suspect transactions, as well as fraud rings. Generally, this layer can also be deployed faster than Layers 3, 4 and 5, and it can be effective in identifying and defeating malware-based attacks.
- **Layer 3** is user- and account-centric for a specific channel (for example, online sales); it monitors and analyzes user or account behavior and associated transactions, and identifies anomalous behavior using rules or statistical models. It may also (optimally) use continually updated profiles of users and accounts, as well as those of peer groups, for comparing transactions and identifying those that are suspect.
- **Layer 4** is user- and account-centric across multiple channels and products (for example, online sales and in-store sales). As with Layer 3, it looks for suspect user or account behavior, but also offers the benefits of looking across channels and products as well as correlating alerts and activities for each user, account or entity.
- **Layer 5** is big data analytics. It enables the analysis of relationships among internal and/or external entities and their attributes (for example, users, accounts, account attributes, machines and machine attributes) to detect organized or collusive criminal activities or misuse.

Source: Gartner Research, G00260461, Avivah Litan, 2 June 2014,

About NuData Security:

NuData Security uses behavioral analysis to prevent fraud online, protecting businesses from brand damage and financial loss caused by fraudulent or malicious attacks.

NuData Security monitors behavior continuously; across every page, and every visit. Fraud is a chain of events, so, by analyzing every visit NuDetect sees the beginnings of fraud the moment it starts - before the transaction.

Businesses achieve improved customer trust by keeping their online brand safe. Reduced costs are realized by lowering reliance on expensive and inefficient security controls such as manual reviews and remediation. The NuDetect platform also allows firms to accept more transactions, with a greater confidence that they will not result in fraud. Operating passively, there is no impact to the user experience.

Head office:
999 Canada Place - Suite 550,
Vancouver, British Columbia,
V6C 3T4 Canada

Phone: +1 (604) 800-3711

Email: bizdev@nudatasecurity.com

Website: www.nudatasecurity.com

LinkedIn: www.linkedin.com/company/nudata-security