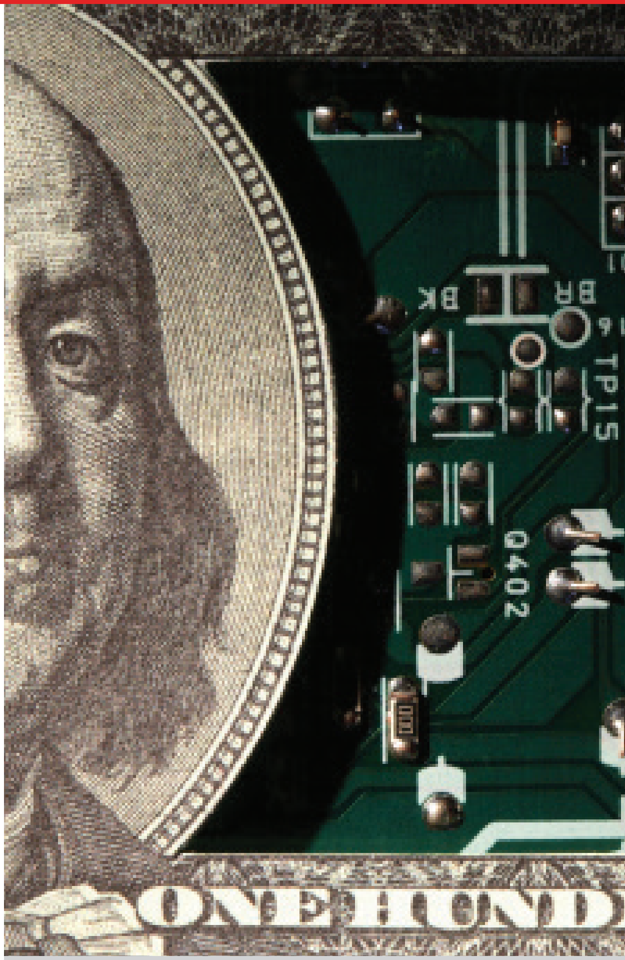
CompTIA

AGMA GLOBAL
Advancing Intellectual Property Protection

WHITE PAPER

IT Industry Warranty and Service Abuse: Stealing Profitability!

Core Issues, New Solutions and Emerging Threats



www.comptia.org

CONTENTS

EXECUTIVE SUMMARY 3

PREVALENCE OF TYPES OF WARRANTY ABUSE ISSUES 4

IMPACT OF WARRANTY ABUSE ON SERVICE PROVIDERS 7

OEM OPINIONS OF WARRANTY ABUSE 11

NEW SOLUTIONS 15

EMERGING THREATS 17

SUMMARY 18

FOOTNOTES & TIMELINE 19

ABOUT COMPTIA 20

ABOUT COMPTIA IT SERVICES AND SUPPORT COMMUNITY 20

ABOUT AGMA 21

- WARRANTY ABUSE STUDY INITIATIVE CHAIRS: 21
- CONTRIBUTORS: 22

ABOUT ZYLOG 23

Executive Summary

“What you don’t know can hurt you.” As it applies to warranty and service, this statement is true for original equipment manufacturers (OEMs), third party administrators, service providers and end users. What you don’t know can impact your ability to be competitive, as well as your bottom line profitability.

This document is the result of a two-year study that included a survey of 402 service providers and 15 OEMs, group workshops and multiple in-depth interviews with industry thought leaders. The research study was conducted by Computing Technology Industry Association (CompTIA) with assistance from Alliance for Gray Market and Counterfeit Abatement (AGMA).

The research study was compiled by Zylog for CompTIA. The results of the study combined assessments of industry experts, reflections on common issues, best practices, and emerging trends that have already started changing warranty processes with a direct financial impact.

Throughout this document you will notice a considerable number of quotes gathered from survey respondents and from comprehensive interviews with industry experts. These quotes are intended to accurately reflect the voice of the industry.

Emerging technology in the form of products, as well as the use of technology for warranty service and controlled costs, is rapidly changing current and evolving trends in warranty service, claims processing, and the end user experience. Highlights of this two-year study are revealed herein, with complimentary action plans and activities for service providers and OEMs.

For service providers and OEMs relying on aging systems, manual processes or reactive responses to issues, this study is a good reflection on the historical challenges and increasing necessity to evolve with emerging warranty and service trends. For companies that may be preparing to establish or enhance procedures in an effort to improve profitability, these action plans and activities are a blueprint and an invitation to “leap frog” over the competition with collaboration, integration and improved practices. For those companies that have been keeping pace, this study provides fresh ideas for creating a roadmap to the future.

PREVALENCE OF TYPES OF WARRANTY ABUSE ISSUES

Warranty and service abuse refers to usage of services, reimbursement for services, replacement of parts or replacement of products to which the client or end user is not entitled.

CompTIA conducted a survey in which 402 Service Providers rated the issues associated with warranty and service abuse.

	Little or No Issue %	Minor Issue %	Major Issue %	Net Issue %
Unnecessary repairs or parts replacement	59	34	7	41
Process or policy abuse	68	27	5	32
False or fraudulent claims submitted to obtain parts	68	26	5	32
Selling extended warranties after warranty period	70	24	5	30
Counterfeit parts	73	20	8	27
False or fraudulent claims submitted for labor not provided	73	22	4	27
Swapping of return parts	74	21	5	26
RMA non-returns	74	22	4	26
Multiple claims on same serial number	75	20	5	25
Reselling replacement parts on the gray market	75	16	9	25
Customer satisfaction surveys falsely completed	78	17	6	22
Counterfeit exchange	80	15	5	20
Claims on stolen or false serial numbers	82	14	4	18
Phantom clients/claims with fake identities	84	13	3	16
Collusion between account manager and the service provider	84	14	2	16
Double billing on replaced parts	85	13	2	15

Fraudulent claims are often attributed to unnecessary repairs or parts replacement.. However, the root cause of the parts abuse varied significantly by product, OEM warranty policies, service provider practices or financial incentives.

Parts Abuse – Process Issues

In some OEM warranty programs there is greater compensation for service based on fewer parts used. For some service providers, there is greater compensation for technician labor based on the use of additional parts in warranty service. The financial incentives from these increased labor reimbursements can have an impact on the decision process during a warranty service event.

As one anonymous survey participant shared, *"Most of our fraud is not with organizations, but with individual employees at the service facility. Once we discover that fraud is being committed and we inform the organization, they are shocked by the activities of the individual. It is most often a matter of controls, tracking and employing checks and balances when money is involved at the repair center. There can be a cost savings for both of us down the road."*

Some forms of abuse are more apparent. In some instances OEMs have identified service providers selling spare parts on eBay and on the gray market — components that were originally ordered for warranty service. In other instances, parts are cannibalized from warrantied products to be used to repair products not covered by a warranty. There are still service providers who attempt to submit fraudulent claims for non-existent clients, even though this type of abuse has become exceedingly easy to identify. While these types of inappropriate activities only pertain to a very small percentage of the service community, the financial impact can be severe and therefore must be contained.

Parts Abuse – Pressure from End Users

Sometimes warranty abuse is related to the timing of parts replacement. On occasion, a part may be ordered as a warranty replacement but it is actually used for out-of-warranty service. As one anonymous survey participant commented, *"I think that the poor economic outlook tempts some service providers to abuse warranty parts programs. When a machine is just beyond the warranty period, pressure applied by 'hard-to-keep' customers is difficult to ignore when new customers are difficult to develop."*

The challenges of controlling abuse associated with replacement parts is further complicated by educated end-users or clients who may be tempted to take advantage of access to information or processes. One anonymous survey participant shared the following observation, *"A big issue we all face is consumer parts abuse problems. End users are getting smarter and know that the OEM uses the same parts in many models. Parts are interchangeable and the manufacturer cannot always track the original part in that specific unit."*

Sandy Ashworth, global director of channel relations and warranty at Unisys, suggests *"I think that part of what is considered warranty abuse many times actually ends up being client and user abuse. A call is received to go out and fix something; we may do the troubleshooting over the phone and then show up with a warranty part to fix it. This is when we figure out that this is a case of customer abuse. When you've ordered the parts you need to get the client up and running, you need to talk to them to understand if this is truly abuse or not abuse. It is an education process at the ASP level about warranty abuse brought about by the actual end user customer."*

Several OEMs reported a problem commonly associated with the replacement of plastic cosmetic parts, particularly at the end of a lease period. Leasing companies frequently charge a fee for replacement of cosmetic parts required to enhance the product resale value. There are sometimes attempts to claim these cosmetic parts as warranty defects, even though the product may be two or three years old and the plastic had been blemished or scratched by the user. Some OEMs ask for samples to audit and some conduct on-site inspections. These checks are an expense for OEMs, and yet it is less costly for them than subsidizing the replacement of user-blemished cosmetic parts.

Counterfeit Parts

Counterfeit part issues are a risk to OEMs, service providers, and end users. These are spare parts or consumables that are produced to look and perform similarly to the original equipment manufacturer parts, but may not actually be tested to conform to the factory specifications. As a result, service providers may acquire a replacement part that appears less costly, but reliability and end user safety may be compromised.

"I don't think it is as much a matter of 'warranty abuse' as it is simply ordering the wrong part or ordering too many parts. The fact that we have provided better technical information has improved the situation."

One example of the impact of counterfeit parts is found in the printer industry with the use of unauthorized ink and toner products. To save money, an end user may purchase delusive ink or toner, unaware that the viscosity and chemical composition of the ink can cause the printer to fail. The end user may then make a request for a warranty repair, but if properly diagnosed by the service provider, it would be identified that the counterfeit part compromised the functionality of the printer, and therefore is not an OEM warranty defect in material or workmanship.

Effective and Evolving Processes

"We get better compliance from organizations that have a warranty claim administrator who manages the documentation and have internal controls to monitor the warranty service technician. It is a check and balance. Service technicians have the ability to order parts and they are under pressure to bring revenue into the organization, so some get creative."

"We've established a strict policy for warranty processing; a second person has to verify that a warranty claim is legitimate. We've also determined that the time involved in processing some claims doesn't warrant the effort required to process a claim. For example, it's actually cheaper to give a customer a replacement keyboard from stock than it is to file the claim on it (tech time, shipping, etc.)," says Scott Storm, president and owner of Storm Computers.

Al Ferrari, senior technical manager at Oki Data Americas, shares one of his company's goals. *"Document as much information as we can; we have a very extensive knowledge base. When you do that, you give the service provider enough information to make better decisions. A lot of times, I don't think it is as much a matter of 'warranty abuse' as it is simply ordering the wrong part or ordering too many parts. The fact that we have provided better technical information has improved the situation."*

One anonymous survey participant shared insight that many OEMs continue to invest in systems and technology to detect and control parts abuse. *"We create equipment to actually detect it, what the human eye may not discover. We've gone as far as creating tools to help us do a more in-depth analysis of returns to see if they have been re-marked or are fraudulent. We also enhance and tighten our checking tools to detect fraudulent claims."*

"Parts first are verified they are defective; all OEM procedures are then followed for processing warranty claims (we strictly manage processes and provide training on how to process warranties). We essentially take control of the assets during warranty and this allows us to be in a better position to service the customer after the warranty (as well as process legitimate warranty claims). We are a parts stocking company, so we have hot spares ready. We then file claim to replenish stock," said Storm.

Simplifying processes can reduce administrative burdens and overhead costs for all involved parties.

OEMs and Service Providers Need to Work Together

There is cost to OEMs to contain warranty and service abuse, and there is also the inconvenience and risk of rejected claims that impact service providers. It is important to prevent this small percentage of fraudulent offenders from gaining a financial competitive advantage based on their improper or illegal activity. "We don't want to put the burden caused from fraud on everyone and that balance is what we have to figure out. Why encumber the 99.9% of service providers who are honest just to find the 0.01% who try to defraud us? That's the balance that we have to strike." said one anonymous survey participant.

By working together to expose and eliminate abuse that OEMs, third party administrators and service providers can reduce costs and improve processes. There are mutual financial interests in identifying, containing and eradicating abuse. Simplifying processes can reduce administrative burdens and overhead costs for all involved parties. It is important to prohibit organizations from gaining a financial competitive advantage as a result of their fraudulent activities, while trying to avoid placing burden on the honest service providers and end users in order to control the risks. This balance can be accomplished by using integrated systems, sharing communications and following other best practices.

Tips:

- Checks & Balances: Segregation of duties, thoughtful incentive programs, thorough documentation and tracking procedures are necessary to prevent abuse.
- Thorough Diagnosis: One of the most effective ways to manage parts cost and abuse is to thorough diagnose and document the failure.
- Customer Satisfaction: End user requests must be balanced against the actual diagnosis and warranty of the product.
- Invalid Returns: OEMs should not assume that the valid defective part will be returned. Verify that the exchanged components are not relabeled, abused by the end-user or otherwise invalid.

IMPACT OF WARRANTY ABUSE ON SERVICE PROVIDERS

As OEMs strive to introduce methodologies to control warranty abuse, it has a residual impact on service providers. That effect is often measured in terms of the administrative costs associated with supporting a variety of complex OEM warranty policies and procedures. An often overlooked, but extremely important, risk for service providers is cash flow. Service providers must pay technician salaries, administrative salaries, overhead costs, parts procurement, inventory and travel expenses upfront, while they await adjudication for warranty reimbursement and risk rejection of their claims.

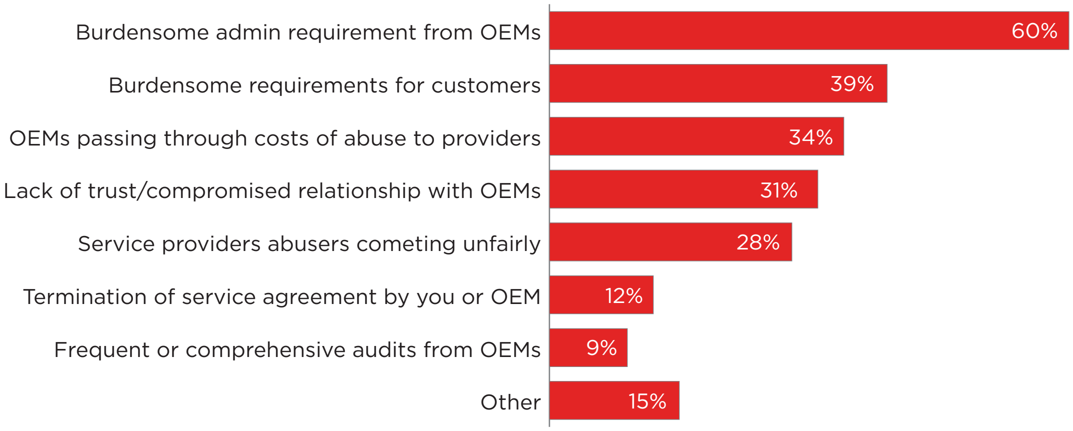
A delayed rejection can be very discouraging for an honest service provider who has incurred costs without being reimbursed for a legitimate warranty claim.

A stringent settlement process enables an OEM to identify and eliminate claims for services for which the recipient was not entitled. These procedures can identify services beyond the warranty period, improper requests for end user blemished cosmetic parts, counterfeit components and individual abuse or fraud. However, the rigorous and diverse requirements may occasionally result in legitimate warranty service claims being rejected due to administrative error, incorrect documentation of details, OEM system mistakes, or human miscalculations. It is especially frustrating when a notice of rejection for a genuine claim is delivered long after the service was completed to the customer's satisfaction. A delayed rejection can be extremely discouraging to an honest service provider who has incurred costs without the being reimbursed for a legitimate warranty claim.

The best process would properly identify legitimate warranty service events and expedite identification of administrative errors or concerns. Effective collaboration and communication between the service provider and the OEM is a necessity to achieve this result.

In a survey conducted by CompTIA in September 2011, service providers indicated the impact of service and warranty abuse on their businesses.

"Because all OEMs do some things a little differently, it is sometimes hard to identify warranty coverage...and that leads to confusion, rather than abuse," observes Levy Antal, executive vice president at Image Microsystems. "Taking care of the client in a timely manner is important to ensure customer satisfaction. Identifying OEM warranty requirements can be challenging and, with a TPA (Third Party Administrator) extended warranty that may have different rules, it can be even more difficult. The rules are not always the same between OEMs and TPAs, especially with regards to the use of original parts, backorders, speed- to- services and costs."



Source: CompTIA Warranty & Service Abuse Study
Base: 394 Service Providers

"Everybody likes options, and that's terrific, but there is no standard set of rules," observes Greg Magee, vice president of business development at LaptopRepair.com. He also adds "What I would really like to see is some sort of standardization."

More than half of the respondents to the survey agree that OEM warranty requirements are burdensome to the service provider, and nearly 40 percent feel that these provisions create a burden on the end user as well. These requirements have been introduced over time,often in direct response to instances or events that resulted in the identification of abuse. Once a method of misuse is identified, an OEM may often create a policy or procedure intended to identify or isolate future occurrences of these issues, and thereby introduce new warranty requirements. Once these changes are made, other OEMs may introduce similar, but slightly modified, versions of the same constraint. Over the years this resulted in a layering of requirements intended to curb warranty abuse. It has also created burdensome administrative overhead for service providers.

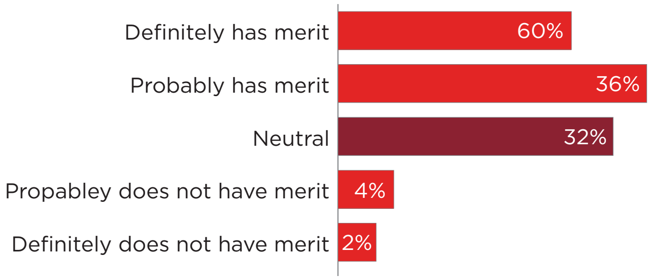
In the words of one survey respondent, *"It would be extremely beneficial for everyone if there was one standard for all manufacturers to adopt and enforce. That would not only make it easier for the resellers to follow, but also easier for those who abuse to be caught."*

In spite of layers of burdensome requirements, 28 percent of respondents still feel that there is an unfair competitive advantage for service providers abusing the warranty process. This reflects a perception that abusers continue to find new ways to circumvent existing controls. It also reveals a perceived competitive disadvantage for providers who invest in the administrative overhead required to do things properly.

Administrative problems can be introduced by any participant in the process and can be the cause for introducing new reasons for rejection in a fluid environment. “One of the biggest problems is getting stuck after the warranty work is completed because the OEM is updating the database at the same time that we are doing the work,” says Antal.

The service providers polled in the survey and in several of the working group sessions agreed about the importance and merit of identifying and controlling warranty abuse. One statement accurately expressed the views of each of the participants, “Remember that we are all on the same side!”

A net 61 percent of service providers see value in OEMs and service providers coming together to develop industry-wide practices and standards (aka, the “common voice”).



Although there is a common recognition that standardization would be beneficial, there are concerns about how the criteria would be implemented, adopted or enforced.

- “Each manufacturer has different rules and policies. It would be hard to get a common voice to accommodate all the different OEMs.”
- “How would it be enforced? The idea is nice, but the people who abuse the system will simply disregard the common voice just as they ignore business ethics.”
- “My only concern is the hoops that we all may need to jump through to be ‘on-board,’ since OEMs will try to weed out the potential abusers with stricter requirements.”

These concerns represent a misconception that creating common standards and common practices would require each manufacturer or service provider to sacrifice its independent systems, practices, or competitive advantages. In fact, this is not the case. Industry-wide practices and standards can be adopted without abandoning important, unique capabilities.

There are already several examples of industry-wide, common standards and practices. These have empowered OEMs and service providers to effectively communicate, collaborate and progress with uniform best practices that did not interfere with individual requirements. Two examples come from CompTIA.

CompTIA has established industry-wide vendor-neutral standards for IT certifications, with its A+ accreditation being one of the first. The CompTIA A+ certification is the starting point for a career in IT. The exam covers the maintenance of PCs, mobile devices, laptops, operating systems, and printers. The CompTIA PDI+ certification covers the installation and maintenance of printing, document imaging and other devices. There are also a number of other industry-wide recognized certifications available from CompTIA. Although these are valued as common standards across the industry for each respective practice, the criteriafor accreditation do not prohibit OEMs from introducing unique certifications and training programs of their own.

A common standard does not dictate a mutually-exclusive practice. Most major OEMs with their own unique training requirements still rely on CompTIA-verified certifications as the fundamental foundation upon which these exclusive conditions are applied.

Another example of creating industry-wide standards that compliment, rather than contradict, independent activity is the adoption of common failure and repair codes. CompTIA developed and encouraged the adoption of RosettaNet PIPS (Partner Interface Processes) that enable OEMs and service providers to communicate by using common industry standard codes for identifying warranty defects (failure codes) and warranty services performed (repair codes). These were rapidly adopted to simplify data exchange, communication and warranty failure rate tracking between manufacturers and providers. Establishing this common set of codes and file structure for communication did not eliminate the independent thoughts, policies or practices of the participants. On the contrary, every contributor continued to conduct service in a unique manner, while the standard format enabled more effective communication. The adoption of common codes reduced administrative errors that may have previously resulted in reject claims, even if they were conducted under legitimate warranty circumstances.

Just as the industry has adopted standards for certification verification, codes and file formats, it can also successfully implement common shared data integration to allow real-time, effective communication between service providers and OEMs. At key milestones in the warranty process, this can significantly reduce abuse, improve processes, enable greater automation and decrease costs for all parties involved.

Today service providers work in a variety of independent systems and environments. They gather information on end users and services and transmitting it to OEMs upon completion of services, with the intention of adjudication and approval for warranty compensation. With the availability of common platforms and technology, it is possible to manage this exchange of communication in association with real-time activities, rather than wait for the entire service to be completed. By addressing the warranty entitlement adjudication from point-of-sale and date-of-purchase to warranty event start and parts procurement, it is possible to provide real-time event adjudication and issue resolutions. That can virtually eliminate erroneous administrative rejections while simultaneously identifying abuse or errors. OEMs and service providers do not need to sacrifice competitive independence to enjoy the benefits of integrated communications and automated alerts.

As a service provider, it is more efficient to work with one internal system and a menu structure designed for their specific business activities and to receive periodic alerts from their OEM.. A technician, without leaving the single sign-on and service menu, may receive the latest service instructions, technical bulletins or recommended repair details from a shared knowledge base. Upon ordering parts, the service provider may be alerted to issues regarding parts availability or components being requested for repair, and how it may affect warranty adjudication or compensation. With advances in current technology, it is easier than ever to know which repairs or parts may be covered by warranty and which are the responsibility of the customer, at every step of the service process.

With a common platform for communication and standard file formats, every participant can work in their system or application of choice. OEMs and service providers can retain their independence while simultaneously leveraging the benefits of shared, timely information and business intelligence. "One way to fix this is to increase open communication and expand

Just as the industry has adopted standards for certification verification, codes and file formats, it can also successfully implement common shared data integration to allow real-time, effective communication between service providers and OEMs..

service provider participation with the manufacturers. That will clear up some of these issues and create a passage for more integrated communications. OEMs need to start pushing out engineering change notices and service advisories quicker, and give their service providers more key indicators,” says Ashworth.

OEM OPINIONS OF WARRANTY ABUSE

CompTIA recently conducted a survey of original equipment manufacturers (OEMs) and ranked the side effects of warranty abuse from high to low, based on the respondents concerns and estimated impact.

1.	Cost in time, staff and resources to “police” abuse
2.	Increased cost of warranty repair
3.	Skews product quality data figures
4.	Damage to brand
5.	Harm to customer experience
6.	Compromises trust with service providers
7.	Good channel partners penalized for the actions of a few bad players
8.	PR challenges/fighting negative perceptions

“The w*hole service business is built on trust,” said Lance Gray of Lexmark. “When somebody does a repair for you and orders parts, you have to take them at their word.”*

Although there was some difference in interpretation, the primary issues identified by the OEMs closely aligned with those identified in the survey of service providers.

Manufacturers expressed great concern with false or fraudulent claims to obtain parts, unnecessary replacement and gray market components. OEMs are also troubled with phantom clients, fake identities, stolen or false serial numbers, and fraudulent claims for services not rendered. These concerns are the result of actual experiences that have caused manufacturers to invest in time, staff and other resources to “police” abuse.

Jim Walters, an experienced director of enterprise business services, explains, *“The program our company put in place is more system-driven and it examines the warranty claim for predetermined indicators of fraud. Parameters are set by our IT team and the system reviews all the warranty bills and tickets that come in under those constraints. At the end of the day it publishes a list of suspect claims, which is examined by a warranty task force which reviews the claims in greater detail. If found to be outside the policy, they are then sent to the field support personnel, who then go to the account to review the submitted claims. Meanwhile, the approval process is put on hold until field support says it checks out.”*

1.	False or fraudulent claims submitted to obtain parts
2.	Unnecessary repairs or parts replacement
3.	Reselling replacement parts on the gray market
4.	Process or policy abuse
5.	Claims on stolen or false serial numbers
6.	Phantom clients/claims with fake serial numbers
7.	Return Merchandise Authorizations (non-returns)
8.	Customer satisfaction surveys falsely completed by service provider
9.	Multiple claims on same serial number
10.	Selling extended warranties after warranty period
11.	False or fraudulent claims submitted to labor not provided
12.	Counterfeit exchange
13.	Double billing on replaced parts
14.	Swapping of return parts
15.	Collusion

The typical processes for policing abuse have historically increased the cost of processing warranty repairs and often compromised relationships with the service provider community. The CompTIA survey of OEMs revealed the most common methods used to combat warranty abuse.

1.	Strong warranty or service policy
2.	Manual Business analytics to detect systemic fraud
3.	Rapid deauthorization of service providers caught or suspected of abuse
4.	Comprehensive audits of service providers
5.	Product registration and tracking systems
6.	Frequent audits of service providers
7.	Automated fraud flagging and prevention
8.	Use of consulting firms with fraud prevention experts

The majority of OEMs surveyed agreed that warranty and service abuse greatly exceeds the cost of implementing strategies and mechanisms to combat these practices. Based on the survey, most of OEMs developed internal practices to police these issues. Despite those measures, every manufacturer agreed that collaboration on standards for communication and common procedures would be practical, require less administrative overhead and allow for greater adoption of best practices.

The historical methods for combating warranty abuse are manually intensive. They require significant administrative reviews, audits, tracking and can result in severe punishment which may include non-payment of service provider warranty claims and de-authorization of suspected offenders. However, by leveraging advancements in technology, the labor and costs associated with the process are decreasing. Walters adds, *“I would say in the past it was 75 percent reactive, but today it is more likely 60 to 70 percent proactive with the monitoring program we have in place.”*

Angela Narvaez, director of brand protection strategy and program development at Hewlett Packard, shared insights on the leading practices her company uses to proactively avoid abuse, rather than relying on “after the fact” audits to recover losses. *“Fraud prevention is really an ongoing process. We leverage a root-cause analysis process for each investigation to understand which process gap or system weakness allowed it to happen. Common themes often emerge, and we have been working for a number of years to build these experiences and information into monitoring capabilities that sit within our entitlement processes. This approach allows us to pick up on red flags before a warranty transaction is processed that may otherwise be caught in detection processes after the fact.”*

Narvaez continues, *“... that is really the direction we are aiming to take the program. We want to shift the paradigm from investigating events after the fact to preventing the fraud before it happens. Once certain abuses or over-ordering occurs you can never fully recover the loss. While you may get partif it back or receive partial repayment, there are soft costs that can never be reclaimed. It’s much more expensive to chase fraud after the fact than to prevent it systematically.”*

We want to shift the paradigm from investigating events after the fact to preventing the fraud before it happens..”

Aaron Woods, director, NARS relationship and partner programs at Xerox Corporation, shares his vision of best practices: *“We try to eliminate warranty abuse at the very beginning, before a claim is submitted and goes through the system. It is important to make sure that the product being serviced has an entitlement (product warranty, extended warranty, or service agreement) and validate it up-front. This should be automated.”*

Woods continues, *“It is important to ensure that the technician servicing the equipment is certified to work on it. This eliminates one reason for claims being rejected. It’s important to do as much as you can on the front end to ensure the submission is valid ... so that all warranty claims in the system are legitimate from the stand point of entitlement and being serviced properly.”*

“It is necessary to have a robust warranty management system that can validate entitlement from the beginning and can authenticate technician certification, so if that claim is processed in a separate system, that tie has to be there,” Woods says. *“On the reconciliation side, we need to ensure that when discrepancies occur, what looks like warranty fraud may in fact be something else that needs to be considered. Some things are not as black and white as they seem, and you need some flexibility to review exceptions. A system that allows that is very important.”“We would like to improve the up-front verification system,”* said Gray of Lexmark.

As one anonymous survey participant said, *“I would like the ability to analyze a claim in process and have the option to give warranty a green light or a red light up front rather than after the fact. This would make it easier to work with our service providers earlier on and avoid rejections or unnecessary charges. Then we would not incur the upfront costs of warranty repairs that never should have been made. Our service providers want the same thing, with software that can accept or deny and give a reason why”.*

The same respondent also shared his views on one of the benefits to OEMs; *"I would like a better failure description of why units need repair. We receive the same reason for multiple machines. Technicians are good at repairs, but do not like to document, so we often do not get the details and information we need."*

Another anonymous survey participant stated, *"The key would be having good integrated data systems to provide as much information as possible on the product across the enterprise and across the company. When someone asksfor information from manufacturing, they should be able to get as much information as possibly available. This will be helpful when they come in to do the return or to claim entitlement. That would help companies identify fraudulent claims. Company tools, infrastructure and databases need to be integrated so that entitlement auditing systems can access as much information as possible to make the most granular checks on the request. My advice is to map out your data streams, from manufacturing to sales to returns, so claims can identify data flow or data alignment across that spectrum."*

"I would like the ability to analyze a claim in process and have the ability to give warranty a green light or a red light up front during the process rather than after the fact."

The hurdles associated with implementing a mutual strategy or common platform include concerns with competitors accessing internal information, ensuring channel partner and service provider participation and addressing the wide variety of current warranty claim processing systems. Recognizing the importance of maintaining confidential, private and competitive information in secure individual databases and systems; the key to collaborative participation and integration is establishing common standards for communicating and sharing vital information. That includes validating warranty entitlement and technician certification, as well as issues that may impact a spare part or warranty entitlement status.

Woods suggests, *"OEMs have the responsibility to give service providers a means to validate entitlement and whether a technician is certified to work on a specific product up-front. These factors should be confirmed and checked at the front end, when the claim is being submitted. This is extremely important."*

Narvaez adds, *"Having a significant impact on this particular challenge will require industry collaboration not only amongst OEM's but also amongst all partners. If we can effectively drive collaboration then we can make important strides in reducing warranty abuse. There are some things that are just more effective in mass, where the wisdom and power of the group make bigger things possible. That is a really important takeaway from this process and something that we must keep in mind as we move forward. We are all competitors (and that's not going to change), but this is hurting a lot of companies, so what things can we do together to make it better?"*

Although OEMs and service providers expressed different thoughts about warranty and service abuse, there is a common interest in identifying discrepancies early on in the claims process.

NEW SOLUTIONS

For service providers and OEMs that have well-established processes, this study highlights the historical challenges. It also offers an opportunity to move forward by replacing aging systems to accommodate innovative and rapidly evolving warranty and service trends. For those preparing to establish or enhance procedures in an effort to improve their profitability, suggestions are a blueprint and an invitation to “leap frog” over the competition with collaboration, integration, and improved practices.

There are a few common points to consider when creating a personal business plan to integrate warranty and communication systems and between service providers and OEMs. Start by embracing the concepts of standard platforms or mutual methods for sharing information that is relevant to your service partner. Common XML formats are a perfect example.

For service providers

- Report point of sale/proof of purchase information to OEMs when the transaction takes place (in the retail environment) to significantly improve the manufacturer’s ability to provide real-time warranty entitlement confirmation and validation.
- Improve communications by providing technician identification.
- Report intended parts procurement or parts usage prior to installation and during the service process to allow the OEM an opportunity to identify potential issues. These problems may include real-time alerts regarding frequency or severity of parts usage, technician or product trends, plastic or cosmetic parts concerns or total cost of service. These issues may also apply to TPA extended warranty claims adjudicators. Common platforms or file formats for communication may permit “real time” alerts and messaging, reducing the risk of perceived warranty abuse or exceptions after the service is completed.

For OEMs

- Improve service provider customer service by providing a common file format for them to request and receive warranty entitlement validation or exceptions.
- Provide technician certification validation to confirm technical training, skills, experience, and tracks the relationship of the technician to the service performed.
- Offer service instruction, technical bulletins and engineering change notices at the time of entitlement and/or technician certification validation to improve quality and speed of service.
- Provide real-time access to service in-process, which enables instantaneous customer satisfaction surveys, immediate review of exceptions for repairs in-process and the opportunity to engage in the claims process. Those procedures may include technician education, warranty adjudication and the ability to associate potential back-order parts delays with specific customers. With this real-time information, the organization is obliged to be an active participant in the service process, which is managed by exception-based alerts that immediately identify, escalate and resolve exceptions.

Most OEMs, service providers and third party claims administrators are expected to collaborate on common industry-wide standards for sharing warranty entitlement, technician certification validation, technical bulletins and parts alerts. It is expected that industry standard milestone events will be established to initiate information sharing, using common file formats. These triggers may include point of sale purchase details, warranty service requests, part orders, engineering change notices and warranty entitlement confirmations. By creating common standards to share this information and identifying the milestone triggers for real-time requests and confirmation, OEMs and service providers will be able to make more informed business decisions. Real-time collaboration will allow all parties to reduce their risks, speed abuse detection and cut down the number of erroneous warranty claims and rejections.

Common standards and milestone events for communication do not sacrifice or prohibit the individual characteristics of OEMs or service providers. On the contrary, every party may continue to maintain their unique systems that provide competitive differentiation, while adding to their capabilities with “turbo-charged, real-time” information.

Creating common standards and milestone events for communication does not sacrifice or prohibit the elegant individualism of OEMs or service providers. On the contrary, every party may continue to maintain individual systems that support competitive differentiation while empowering the individual systems with turbo-charged real-time information.

As the technology and systems for collaboration continue to evolve at an astounding pace, the devices and applications purchased by end users also continue to advance, further modifying the environment for warranty claims and service. *“Providing service providers with valid communication processes and tools would allow them to better follow OEM guidelines, a key to preventing warranty abuse,” according to one survey respondent. “As OEMs, we need to trust our service providers, provide them with accurate communica*tion and information, and provide them with guidelines in a single, precise location.”

Among the most prevalent forms of reported warranty abuse are parts usage issues, unnecessary part replacement, false or fraudulent claims to obtain components, gray market parts and end user abuse. However, the growing number of products with no mechanical or moving parts are not as susceptible to heat or extreme temperatures. These products are more rapidly discarded and replaced, and rarely repaired, so the demand and availability of parts in proportion to product are expected to change dramatically over the next three years. With the increased interest in tablet devices, use of touch screens rather than keyboards, and reduced reliance on hard disk drives, there will be significantly fewer parts to replace. Smartphones have become a dominant form of communication, used for much more than telephone conversations, and are easier to exchange than they are to repair. With this shift, spare parts are likely to become less of a concern for IT warranty abuse.

Emerging Threats

There are always new threats on the horizon. The next technical revolution may be as significant and rapid as the journey from PCs to tablets. Many of the emerging devices rely heavily on distributed computing, external storage and cloud computing. The next developing concern for warranty abuse may not be from gray market parts, but from data pirates. Protecting customer data, privacy, mobility and information abuse are predicted to place new pressures on OEMs and service partners over the next several years. These new concerns should addressed in every company’s warranty and service action plan.

“Data piracy and protection will become more of an issue as companies secure what they keep in the cloud” says Narvaez. “I predict that we will see the landscape change significantly, as more customers access their systems and information via terminals or mobile devices. As this occurs, part returns will drop substantially while internal system maintenance (inside IT companies) will increase.”

Another emerging trend that OEMs and service providers should keep in consideration is 3-D printing. As the technology continues to develop into a more commercially-viable process, with lower costs and lower prices, it will permit the duplication and reproduction of many cosmetic parts. 3-D printing will have a substantial impact on the manufacturing industry, service providers, patent laws, parts accessibility and warranty plans. It may become a more cost-effective process for producing replacement cosmetic parts, plastics and bezels on-demand. Rather than investing heavily to maintain aging equipment or to carry an excessive amount of inventory, companies can produce these pieces only when needed using a 3-D printer.

As with the changes resulting from advances in the cloud and 3D printing, unplanned threats may come from unexpected sources. The insight needed to properly prepare for potential threats is often the result of effective communication and collaboration with industry peers and innovators.

“For more than 30 years CompTIA has represented with great foresight the interests of the world’s IT industry; from the companies at the forefront of innovation to the workers who turn innovation into real business solutions that help organizations maximize the benefits they receive from technology. Our industry faces great challenges; economic and employment, environmental and educational. But we also have a great opportunity to demonstrate how technology can help to better our world. Together with the CompTIA Board of Directors, our worldwide membership and our professional staff, I look forward to meeting these Todd Thibodeaux, President and Chief Executive Officer at CompTIA.

SUMMARY AND RECOMMENDATIONS

As a result of a two-year study that included a survey of over 400 companies, numerous focus groups, and four months of in-depth interviews with industry thought leaders; CompTIA and AGMA produced a well-defined analysis of issues impacting original equipment manufacturers (OEMs), service providers and third party administrators. The results of the study reveal tangible methodologies and approaches to substantially improve the state of the industry with regards to warranties, their related processes and communications. The recommendations are best practices based on the rapid evolution of the industry and end user products, supporting the notion that adaptation is a necessity for competitive survival.

- Service providers and OEMs must work together to improve processes and communications. The best results are achieved through collaborative efforts.

- Service parts usage results in numerous types of abuse. The best outcomes are achieved by using OEM controls for parts identification and by implementing clear end user rules. Service providers can achieve the greatest results by employing internal warranty claim administrators who monitor end user and technician part usage and procedures.

- Interactive or integrated communication during the warranty process can reduce errors, improve customer service and reduce or eliminate the risk of warranty rejections that often occur long after repair is completed. Some key information that should be shared and communicated between OEMs, resellers, service providers and the TPA includes:

  - Date of purchase
  - Date service requested
  - Warranty status of product
  - Warranty technician ID dispatched or assigned
  - Technician ID certification verification
  - Technical instructions, service bulletins, history of repairs by unit
  - Suggested parts
  - Date parts requested
  - Part numbers requested
  - Warranty by part, or potential issues (cosmetic plastic parts, etc.)
  - Exception, authorization and error handling
  - Date service completed
  - Customer survey

- Standard file formats allow service providers and OEMs to communicate in “real time” during each milestone step of the warranty process. This lets manufacturers rapidly determine if they lack information regarding a warranty process or if they have a case of potential warranty abuse or an exception. Communication during the service process enables service providers to provide real-time responses to end users and make informed decisions regarding these procedures based on details provided by the compensating OEM.

- These standard file formats (for communicating during service events) allow each manufacturer to maintain independent internal systems and processes. They also let each service provider use its servicer software of choice for maximum flexibility and operational efficiency, while all parties can leverage the benefits of real-time business intelligence.

- A proactive approach to service administration, communication and technology is a necessity since a reactive process for service abuse or rejected claims can be costly, time-consuming and risky. OEMs need effective integration between product manufacturing, registrations, parts usage, sales, and other internal systems to maximize prevention and identification benefits.
- Real-time visibility increases trust between the parties involved which is essential to delivering satisfactory and cost-effective customer service.
- Emerging technology will have an increasing greater impact on warranty service trends. With lower cost products, data stored remotely in the cloud, rather than on a device, and solid state systems, demand for spare parts will decrease while the complexity of storage will simultaneously increase. Warranty issues related to data will become more prominent as BYOD (bring your own device) introduces new complexities to the network while reducing corporate warranty claims.
- OEMs and service providers each benefit by collaborating on standards for warranty validation, real-time communication file formats and technician certification verification. All parties may maintain some of their own, unique systems or business rules, provided each can accommodate a uniform method of effective real-time communication and integration.
- Suggested next steps for the industry include working on standards for communicating the most common relevant data elements needed for warranty validation, technician certification verification, repair event milestones, exception identification and error handling.

FOOTNOTES & TIMELINE

- The CompTIA Warranty Service and Abuse Survey was conducted as an online survey in September 2011. A total of 402 companies participated in at least one portion of the survey, yielding an overall margin of sampling error at 95% confidence of +/- 5.0 percentage points.
- An online survey among a focus group of 15 original equipment manufacturers (OEMs) was conducted in September 2011.
- Perspectives of survey results were analyzed by focus groups and the CompTIA IT Services and Support Community members in January and March 2012.
- Focus groups for best practices were assembled by CompTIA at the Annual Members Meeting in March of 2012 and at the Breakaway (now ChannelCon) conference in August, 2012.
- In-depth interviews with numerous industry thought leaders were conducted from January through April, 2013. Some industry thought leaders are quoted in the report findings, others are mentioned as contributors, and several more participated in interviews where they could not be identified by name/company name due to individual corporate policies. Nevertheless, even if not mentioned specifically, the contributions of all individuals in the surveys, focus groups and personal interviews are reflected in this document.

ABOUT COMPTIA

CompTIA is the voice of the world's information technology (IT) industry. As a non-profit trade association advancing the global interests of IT professionals and companies, we focus our programs on four main areas: education, certification, advocacy and philanthropy.

We:

- Educate the IT channel: Our educational resources, comprising online guides, webinars, market research, business mentoring, open forums and networking events, help our members grow their businesses and become "best in class."
- Certify the IT workforce: We are the leading provider of technology-neutral and vendor-neutral IT certifications.
- Advocate on behalf of the IT industry: On Capitol Hill, we bring the power of small- and medium-sized IT businesses to bear as a united voice.
- Give back through philanthropy: Our foundation enables disadvantaged populations to gain the skills they need for employment in the IT industry.

Our vision of the IT landscape is shaped by 30 years of global perspective and more than 2,000 members and 2,000 business partners. We are driven by our members and led by an elected board of industry professionals.

All proceeds are directly reinvested in programs that benefit our valued members and the industry as a whole. Headquartered outside of Chicago, we have offices in the United States, India, Japan, South Africa and the United Kingdom.

ABOUT COMPTIA IT SERVICES AND SUPPORT COMMUNITY

The CompTIA IT Services and Support Community provides a forum for IT services industry executives to meet and discuss commonality within the service and support business.
This collaborative group crafts industry standards, best practices and initiatives; provides networking opportunities among IT services thought leaders; develops industry-specific education and tools; and enhances the services industry's quality and productivity

ABOUT AGMA

AGMA is a unique alliance of intellectual property (IP) rights holders, with members' combined annual revenues in excess of $425 billion, who recognize that IP protection is a fundamental element of innovation and economic growth. AGMA's members are some of the most innovative technology companies in the world, investing millions of dollars in local economies and developing branded products trusted by billions of people.

Building on the extensive knowledge of our members, AGMA further develops IP protection concepts, educating the industry, law and policy makers, and end users in order to transform these concepts into best practices. These best practices can be used to combat four distinct threats to the high-tech industry: (1) gray marketing; (2) counterfeiting; (3) service and warranty fraud; and (4) unauthorized use and/or distribution of IP in a digital format (digital IP).

Since its incorporation in 2001 by 3Com, Cisco Systems, Hewlett-Packard, Nortel and Xerox, AGMA has participated at many industry conferences, raising awareness and educating the industry on the serious issues of gray market and counterfeit technology - and the impact on end users and the high-tech industry as a whole. AGMA has submitted testimony for a Congressional hearing on the economic impact of gray marketing and counterfeiting, and has steadily and continuously grown its membership base.

AGMA focuses on raising awareness on related issues by sharing our studies and best practices, and by providing a platform for open sharing of information.

Warranty Abuse Study Initiative Chairs:

Aaron Woods

Director, NARS Relationship and Partner Programs at Xerox Corporation

Aaron Woods is the director of North America Resellers (NARS) service programs in the Services Partners and Alliances (SPA) support group, a part of the Xerox Services (XS) organization. Some of his primary responsibilities include developing partner programs targeted at increasing post-sale revenue and maintaining customer satisfaction.

Outside of Xerox, Woods is actively involved in industry initiatives targeted at improving the service offerings and experience of Xerox Authorized Service Providers. He was instrumental in helping to develop and introduce the CompTIA A+ certification program for technicians in 1993. He has served as chair and vice chair of the A+ Certification Advisory committee and is currently the chair for the PDI+ committee. In July 2007 Woods completed his Green Belt certification for Lean Six Sigma (LSS) quality improvement processes. His current focus is targeted at implementing Printer and Document Imaging (PDI+) technicians that was introduced in January 2008.

Woods is a result-oriented, customer-focused senior executive who excels at building strategic alliances with organizations and leaders to effectively align with and support key business initiatives. He builds and retains high performance teams by hiring, developing and motivating skilled professionals.

Sandy Ashworth

Global Director, Channel Relations and Warranty at Unisys

Sandra Ashworth has been in the IT services industry for more than 25 years in various capacities such as field management, operations, vendor relations, customer service design/implementations, and supply chain marketing. She presently represents Unisys Corporation—where she is the global director of channel relations and warranty—at CompTIA meetings. Ashworth has been the chair of the IT Services and Support executive council for more than seven years and is presently chair of the Advancing Women in IT community. She has been a member of CompTIA for more than 20 years. Through the association's initiatives, she believes industry contributors will realize a return on their investment by delivering better quality services and cost reductions, whether they are a global or regional channel partner.

Angela Narvaez

Director, Brand Protection Strategy & Program Development at Hewlett-Packard

Angela Narvaez is the director of brand protection program strategy and development, a part of the Hewlett-Packard Global Security Group. In this role she shapes the future direction of initiatives to combat theft, counterfeiting and fraud. These initiatives build on the expertise of our investigative teams taking our learnings upstream with the aim of preventing crimes involving our products and processes. This work includes proactive analytics of market transactions, investigation of product/process abuses, development of investigative intelligence, and coordination with business teams to implement transformative system protections and process improvements.

Prior to managing brand protection strategy, Narvaez held a number of positions covering security operations, anti-counterfeiting, workplace violence, and supply chain security. All of these programs are part of a suite of proactive security programs in Hewlett-Packard's Global Security Group. Narvaez currently serves on the board of AGMA Global and leads the warranty advocacy helping to develop best practices for the industry.

Contributors:

- Levy Antal – Image Microsystems
- Sandy Ashworth – Unisys
- Al Ferrari – Oki Data
- Lance Gray – Lexmark
- Greg Magee – LaptopRepair.com
- Angela Narvaez – Hewlett-Packard
- Charlie O'Shaughnessy – Intel
- Scott Storm – Storm Computers
- Jim Walters
- Aaron Woods – Xerox

ABOUT ZYLOG

Since 1995 Zylog has been a leading provider of technology solutions, human capital resource management, and IT and engineering professional services that help enterprises achieve the outcome they desire in order to succeed. By offering business intelligence, retaining top talent with unique services for the professional community and delivering innovative integration with thought leadership, Zylog empowers clients and partners to exceed expectations in their own respective competitive landscape.

Contributors from Zylog:

- Carlotta Dormiendo
- Doran Foeller
- Kim Jacot De Boinod
- John Mehrmann
- Mike Schuler
- Chiara Shmayda

How Zylog can help:

- Assistance in the development of communication formats, files and event triggers
- Assistance in the development of a warranty service abuse prevention program
- Service provider management systems, field service management systems, CRM, warehouse management, split claims adjudication, technician management, etc.
- Integration with third party administrators and systems, data migration and consolidation
- Assistance with technician certification validation
  www.Zylog.ca
  Toll Free US and Canada: 1-877-432-7246

CompTIA®

AGMA GLOBAL
Advancing Intellectual Property Protection

www.comptia.org

www.agmaglobal.org

CompTIA Worldwide Headquarters
CompTIA Member Services, LLC
3500 Lacey Road, Suite 100
Downers Grove, Illinois 60515
630.678.8300

AGMA Global
15466 Los Gatos Boulevard
#109-167
Los Gatos, CA 95032
252.500.0123