Service blues

Effectively managing the multi-billion dollar threat from product warranty and support abuse

Table of contents

Executive summary
The critical importance of managing warranty service abuse

Study results confirm service abuse activity is estimated to result in a **3 to 5 percent loss in revenue alone** ($10 billion for just the survey participants), with total loss exposure even higher as companies often struggle to quantify all of the implications of entitlement abuse.

"Warranty service abuse is a significant global problem that is disruptive to businesses and is perpetrated by increasingly innovative means. The consequences of the abuse are significant and can include degradation of customer confidence and company reputation, increased cost of providing services, loss of service revenue, increased gray market activity, loss of new product sales and increased R&D costs."

Ram Manchi
AGMA® Director and President

Facing badly bruised credit and financial markets, a sluggish economy, and the obligation to grow or even stabilize revenue and rein in costs, businesses must be keenly aware of threats to business performance and reputation.

With much of the world still reeling from the economic downturn, PricewaterhouseCoopers (PwC) and the Alliance for Gray Market and Counterfeit Abatement (AGMA®) have highlighted a significant financial drain about which many companies remain unaware: abuse of warranty and product support entitlements ("warranty service abuse" or "entitlement abuse").

PwC combined its extensive risk and controls knowledge with AGMA® members' first-hand insights into the warranty service abuse faced by the technology industry to develop a thorough analysis of the abuse worldwide, and to identify opportunities for curbing the ongoing threats arising from this form of entitlement abuse.

PwC conducted surveys and extensive executive interviews of AGMA® membership—a bellwether for the technology industry—and other notable technology companies. These efforts, which were further supported by PwC research, insights, and experiences, yielded results that may be surprising: **warranty service abuse costs businesses billions of dollars that could be significantly reduced with appropriate vigilance and controls.**

Beyond the costs and lost revenues associated with servicing invalid claims, additional damage can be done to a company's reputation and brand. Likewise, relationships can be impacted with business partners who are effectively penalized for "doing the right thing" regarding warranty and service programs, as they may compete unfairly with unethical opportunists who may have profited from fraudulent schemes.

Some companies may choose to write off the losses from warranty service abuse as a cost of doing business, unwilling to risk any negative impact to legitimate customers by addressing abusive activities. However, **companies that address warranty service abuse can generate enormous savings and create long-term value for their organizations, their investors, and their customers, without compromising customer service and satisfaction.** Getting a handle on prevention necessitates executive-level buy-in, enterprise-wide action, and risk mitigation through practical controls, enforcement efforts, and appropriate messaging.

Our analysis is intended to expose the multi-billion dollar threat arising from entitlement abuse, and more importantly, provide tools and insights to help manufacturers implement practical mechanisms to prevent or detect entitlement fraud—while maintaining the level of service delivery demanded by customers.

Top abuses, vulnerabilities, and safeguards

Top five forms of warranty service abuse*

1. Non-returns or advance replacement exploitation

2. Claims by third-party service providers for services never performed

3. Under-coverage (misapplication of coverage)

4. Just-in-time coverage

5. Buy one and sell several

Top five vulnerabilities

1. Inadequate entitlement verification

2. Weak user authentication

3. Poor management of returned merchandise

4. Improperly input base data (sale, service contract, serial number)

5. Lack of control or visibility into third-party service providers

Top safeguards

1. Active serial number utilization and verification

2. Utilization of continuous monitoring such as computer assisted auditing techniques (CAATs)

3. Clearly communicated guidelines, expectations, and policies

4. Active and consistent enforcement (through contract compliance audits, investigations, and prosecution of perpetrators)

5. Enhanced controls for complex or high-value transactions

* See warranty service abuse schemes detailed within the section: Case Studies in Entitlement Fraud

What is warranty service abuse?

Warranty service is post-sale support delivered (over a defined period of time) by manufacturers[1] to the end-customer to enhance or provide added value on products purchased. **"Warranty service abuse" refers to usage of services or replacement products to which the customer or recipient is not entitled.** For example, acquiring a service contract for some products, and using that service contract to request and receive service on a product not covered by the contract would represent warranty service abuse. Likewise, requesting a replacement for a product not owned or not returned by a claimant would represent warranty service abuse. For purposes of simplicity within this paper, we do not differentiate between warranty abuse and service abuse, which differ in timing and application (i.e., abuse of standard warranty versus abuse of a service plan), often because the frauds perpetrated are similar, as are the control solutions employed to curb the abuses.

The abuse can be as simple as a customer requesting warranty service on an expired service plan, to the sinister and complex. Consider Apple's recent $2.5 million loss[2], in which the fraud was predicated on an outright lie. In this case, Apple alleged that a reseller group charged its customers a fee for replacing products not covered by warranty or service agreements. The resellers then submitted those damaged products for replacement to Apple, using serial numbers for different products known to be covered under valid warranty or service agreements.

Other fraud schemes involve targeting software and technical support whereby service abuse serves as a backdoor means of obtaining unlicensed software or replacement goods and services.

A detailed description of various common abuse schemes can be found in the entitlement fraud case studies section later in this paper.

---

1   Authorized representatives or business partners such as distributors, resellers, integrators and third-party servicers may also deliver post-sale support on the manufacturer's behalf

2   www.channelnews.com.au/Hardware/Mobility/M9Q4F7K5.

Warranty service abuse is on the rise and threatens performance

Of survey respondents, 93% agree or strongly agree that the issue of service abuse has become more important over the past five years, and 91% believe the issue will become even more important over the next five years.

In the aggregate, entitlement abuses relating to warranty service **cost US businesses billions of dollars** each year, according to the information gathered by the PwC-AGMA® study. However, the total cumulative cost of warranty service abuse is tough to nail down for various reasons, most notably the lack of consideration of the many implications of the abuse (see implications of warranty service abuse on page 8).

Even companies that successfully root out and prosecute warranty service abuse have difficulties estimating its costs. Consider the difficulty faced by IBM in 1993 when rectifying a weakness that had been exploited: the company attempted to estimate the total cost of a warranty scam perpetrated by its dealers, with loss estimates ranging from tens of millions to hundreds of millions of dollars[3]. The issue and implications are nothing new, and the absence of real industry-wide efforts to mitigate the threat appears to encourage more egregious fraud examples.

Survey 1: Areas impacted if service abuse was discovered at your company (% respondents agreeing)

Area	%
Financial loss from unentitled service costs	74%
Loss of service revenue	68%
Failure rate distortion- increased R&D cost	65%
Enforcement costs	61%
Brand compromise	55%
Loss of new product revenue	52%
Serial number compromise	52%
Customer confidence degradation	45%
Dissatisfied distributors—impact on their cost and margin	42%
Contamination of service part supply chain	35%
Operational interruption	35%
Corporate reputation on operational inefficiencies	32%

---

3   http://query.nytimes.com/gst/fullpage.html?res=9F0CE7D81331F933A0575AC0A965958260

PricewaterhouseCoopers LLP

Further complicating total loss estimates, companies offer different warranty and service coverage, operate in diverse global regions, and employ a variety of prevention programs.

Some of these impacts may be difficult to quantify, but service abuse activity is estimated to result in a **3 to 5 percent loss in revenue alone**. In other words, lost revenues were estimated at approximately $10 billion for just the survey participants. Based on our research and experience, amounts tend to be underestimated, as companies often struggle to quantify the extent of the issue and may not consider all of the implications of abuse. For example, this estimate does not include the various costs associated with servicing invalid claims, or the damage to brand reputation or business relationships caused by the abuses.

Survey 2: How much revenue do you think the company loses due to "service abuse"?

0%-0.5%	13%
0.5%-1%	20%
1%-5%	47%
5%-10%	13%
Above 10%	7%
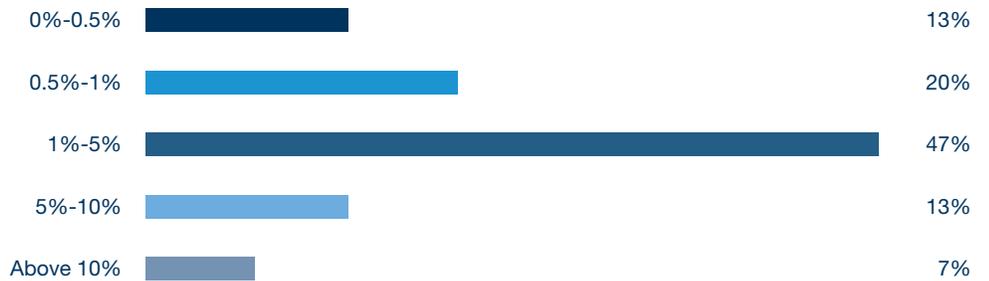
Impact of warranty service abuse

Warranty service abuse can impact the company's profitability in a number of ways:

Revenues

- Loss of revenue due to under-coverage (i.e., customers don't buy a service contract for all products but expect to receive coverage on all purchases).
- Downward price pressure and revenue loss resulting from products obtained through service abuse and sold on the gray market.
- Unauthorized software download and lost revenues or licensing fees from software support abuse.
- Unauthorized revenue transfer to distributors and third-party servicers who sell service plans separately without compensating the manufacturer.

Costs

- Costs of providing un-entitled services, including responding to invalid claims (e.g., technician visit related time and materials or call center support).
- Costs to receive, process, and service non-covered products or components (especially heightened when distributors/resellers have lax return policies).
- Costs of actual replacement products shipped without valid entitlement.
- Distorted product failure rate statistics, and the impact on R&D costs.
- Loss of product through scrapping returned products due to questionable source or quality.

Relationships

- Decreased service levels for valid service claims (service provided to un-entitled customers can delay legitimate claims and deplete the inventory of parts on hand at your service depots).
- Participation in service abuse by some business partners creates an unequal environment for ethical business partners, as fraud perpetrators can unfairly leverage the benefits from their activities.

Reputation

- Reputational risk, loss of consumer confidence, and a compromised brand can occur due to negative press and public perception of poor product quality and diminished service levels.
- Tacit acceptance of counterfeit or gray market products "washed" through a company's warranty service function encourages further abuse.
- Fraud perpetrators share strategies, meaning weaknesses are further exploited through increasingly sophisticated techniques, exacerbating the problem and implications.

Sources of entitlement abuse

The perfect storm

The Fraud Triangle, developed by the criminologist, Dr. Donald Cressey, describes three conditions that are commonly found when fraud occurs. The perpetrators experience some *Incentive* or *Pressure* to engage in misconduct. There must be an *Opportunity* to commit fraud and the perpetrators are often able to *Rationalize* or justify their actions. The global economic decline is such that each of these three factors (*Incentive/Pressure, Opportunity* and rationale) is present as never before.
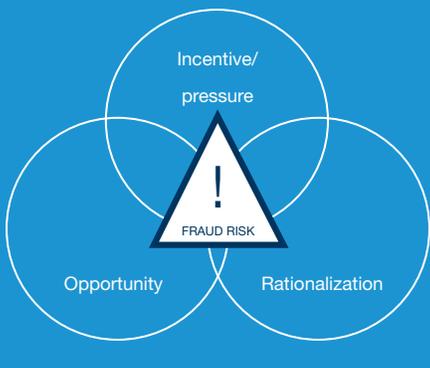
To thwart the threat and implications of warranty service abuse, it is important to understand who the perpetrators are.

Based on our research, business partners, including third-party service organizations and distributors/resellers, are the parties most likely to abuse the entitlement process. They typically have access to valuable information such as service contract numbers, and product serial numbers which can be used to exploit control weaknesses in servicing claims. However, as many manufacturers' primary point of contact with customers, they also can be one of the greatest allies in curbing the abuses for these very same reasons.

In addition to business partners, entitlement abuse perpetrators also include organized crime and career criminals who make a living on warranty service abuse.

Entitlement abuses by unethical end-users are also significant through under-coverage schemes, and coverage acquired after the product stops working properly. It is noteworthy that although warranty service abuse is generally conducted intentionally and illegally, these activities can also ensnare innocent consumers who make honest mistakes. This type of service abuse can have many causes, including lack of customer education on what constitutes valid service coverage, and misrepresentation by business partners who sold the product or service plan. This is especially true in particular regional markets. For example, in some Asian markets the consumer commonly believes extended warranties and service should be provided automatically, as it is presumed to be built into the product price.

Survey 3: Who commits service abuse? (% respondents agreeing)

Partners/resellers	87%
Small/commercial customers	74%
Petty criminals	65%
Organized criminal groups	61%
Employees of customers/partners	52%
Enterprise customers	48%
Independent consultants	16%
Governments	10%
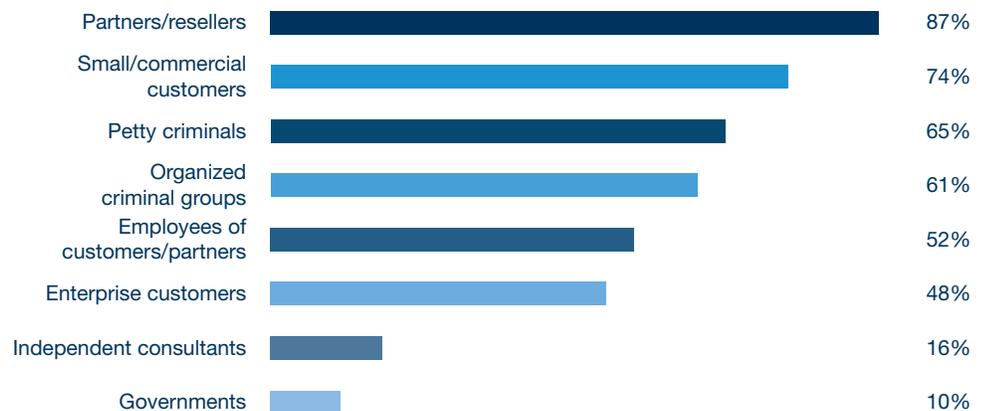
Case studies in entitlement fraud

> "Globalization is an issue that companies continue to confront as they try to control this issue. Companies must ask themselves what it means in terms of the old methodologies for identifying entitlement, and how you confront the issue when your business partner is in another part of the world."
>
> Tony Savastano
> VP of Customer Services–Finance
> Cisco

Warranty service abuses come in many forms. The following case originated from gray-marketed products traced back to warranty service contracts. This case demonstrates various frauds that can be employed as part of complex warranty service abuse schemes:

HP filed a nearly $2 million lawsuit in 2003 alleging a conspiracy to fraudulently obtain equipment and parts for warranty repairs that were subsequently sold on the gray market. The computer giant informed a business partner that pursuant to their agreements, HP had selected the company for a compliance audit. HP alleged that at least 90 percent of warranty claims the company had submitted were fraudulent and/or not in compliance with the terms of agreements and program requirements. Audit evidence confirmed that:

- false or invalid warranty claims were submitted to obtain parts;
- false claims were submitted for labor not provided;
- false customer names or account information was provided;
- customer satisfaction surveys were falsely completed on behalf of nonexistent customers;
- replacement parts were resold on the gray market.*

Source: http://www.crn.com/it-channel/18831000

As varied as the implications of warranty service abuses, or the differences in the perpetrators, an equally diverse and complex number of frauds have been perpetrated.

Survey 4: Forms of service abuse believed to be prevalent among global companies (% of respondents agreeing)

Form	%
Counterfeit exchange	69%
RMA non-returns	69%
Over-usage	66%
Large contract abuse	50%
Multi-level service abuse	50%
Scrap/lease returns	44%
Buy one, sell several	31%
DoA non-returns	28%
Under-coverage	25%
Contracts & ID theft	22%

The following are some examples of the most prevalent frauds committed:

Under-coverage: "What's good for some is good for all"

Under-coverage occurs when a customer purchases a small number of (often premium) service contracts, or a contract that covers specific products, and attempts to overuse that service (or replacement offering) on products that don't carry the same level of coverage.

In some cases, technicians performing the service may realize the product isn't covered, but they perform the requested service anyway, rationalizing that they are already at the service site, and that the customer may have made an honest mistake. Either way, the cost associated with the visit, and the potential delays in service for legitimate claims, are real.

Non-returns or advance replacement exploitation: "You'll get it any day now…"

Non-returns are one of the most common of the warranty service abuse scams, and a major source of gray-market goods. In this fraud, perpetrators submit single or multiple requests for replacement products on a warranty or service contract[4] while never sending back a covered product, thus acquiring an inventory of product for free.

In many cases, the perpetrator sends nothing back, or may return scrap, a different product, or even counterfeit product. The fraud will often vary based on the types of advance replacement programs offered by the manufacturer, and the return management processes and controls the company has in place.

Just-in-time coverage: "*Now* I'd like to talk about that service contract…"

In this very common abuse scheme, the customer fails to purchase a service contract for the product at the time of original purchase. Instead, the customer waits until a product breaks down to purchase a service contract for it. A short time later, the customer makes a claim for service on the product using the newly acquired coverage.

Buy one, sell several: "There's plenty to go around"

A favorite for unethical third-party service providers, this abuse occurs when a service company buys a small number of valid service contracts, then re-sells their own service agreement to several customers. Knowledgeable of product serial numbers or other identifiers, the servicer submits claims to the manufacturers for the covered products, for service work actually done on products sold without valid service plans.

---

4   Return merchandize authorizations, or RMAs, and often non-functional products sent to end customers ("DoA"), are usually covered under advanced replacement premium support contracts

In the process, the revenue from service plans is passed from the manufacturer to the fraud perpetrating service provider. Furthermore, the manufacturer often incurs additional costs due to the replacement of products that are not properly covered under contract.

Fraudulent service claims: "You won't even know we're here"

As described in the earlier HP example, in this fraud a third-party servicer uses valid serial numbers and other customer information to submit claims/invoices for services not actually provided.

Simple service abuse: "Just an honest mistake"

As the name implies, this technique simply involves a customer who submits a service request or requests a replacement for un-entitled products; the request is fulfilled because of insufficient information to refute the claim, or a decision is made to fulfill requests regardless of entitlement coverage.

Software download key abuse: "Our guests act like they own the place"

Service abuse also affects software. Some customers or perpetrators take advantage of customer-centric but poorly controlled web-enabled services. For example, a company may purchase a software service agreement for one piece of software to gain system access, and then downloads additional software for which no payment or license fee has been made. Similarly, an authorized reseller with access to a licensing system may abuse it to provide licensing (usually for a fee) to unauthorized resellers or other parties that have not obtained a valid license.

Survey 5: Enablers of service abuse (% of respondents agreeing)

Enabler	%
Inadequate entitlement verification	84%
Systems/tools vulnerabilities	69%
Weak user authentication	69%
Poor returns management	62%
Questionable installed base data quality	62%
Deficiencies in policy, process and/or practice	56%
Lack of service history at serial number or device level	53%
Inability to track service on scrapped parts	47%
Lack of licensing controls	41%
Weak asset recovery	41%
Lack of account team engagement/management	34%
Limited controls for data access	34%
Inconsistent delivery models	31%

Control weaknesses that often enable warranty service abuse:

- Business cultures that allow it, or disregard its impact

- Failure to match serial numbers of products being serviced or replaced with those under valid service contracts

- Lack of monitoring to confirm that customer returns (e.g., RMAs) are made on a timely basis, and that products returned are actually covered products

- No collateral received prior to providing advance replacements

- Advance replacements provided without appropriate justification, entitlement, approvals, etc.

- Lack of appropriate entitlement tracking (i.e., information systems cannot quickly confirm which products and respective customers are entitled to warranty service coverage)

- Lack of service history tracking at a serial number level, customer level, etc.

- System controls do not prevent the download of unauthorized software

- Software controls do not require the registration of software before it is activated for use

- Lack of certification processes and compliance monitoring (including contract compliance reviews) of third-party service providers and distributors, resellers, etc.

- Access to valid serial numbers listings by external parties or those without a valid need to know

- Weak contract monitoring and linkage to service systems, such as failure to differentiate active versus expired service contracts

- Poor product data management (such as failure to track valid product and serial number configurations)

- Lack of analytics and assessments on sales and claim-related data

- Poorly designed contract terms

Implementing an effective entitlement abuse prevention program

Effectively reducing warranty service fraud requires patience, knowledge, and deep commitment. A holistic, end-to-end approach to implementing a prevention program includes factors that will likely influence your efforts to manage common threats encountered, including recommendations for how your business can implement efficient processes and controls.

1. **Commit to change**

   Company leadership should identify a change catalyst to lead the charge within the organization. We recommend this person or group first understand where the company is exposed, where and how abuse schemes have festered in the past, and how they can best leverage the recommendations in subsequent steps in the framework to remedy those deficiencies. Next, working with management, the individual or group takes responsibility for developing warranty service polices and related programs.

2. **Program communication**

   Once a policy and related program is developed, it should be communicated to stakeholders—executives and employees, then externally. The business formally notifies business partners, third-party servicers, and its largest customers of the rules of the road governing prohibited activities and required business practices. Business partners who serve as intermediaries with customers, or with whom customers have the direct relationship, are also encouraged to reinforce warranty service policies, along with the value provided through a valid service entitlement.

3. **Build a culture of compliance and risk management**

   AGMA® feedback suggests that most service abuse was identified by internal controls and quite frequently reported by employees through appropriate channels. But in the absence of an entity-level, enterprise-wide commitment, the business will remain vulnerable, sending a dangerous message to would-be perpetrators.

   Thus, executive buy-in is critical to set the tone at the top. It is also frequently the initial and most significant hurdle for many organizations striving to add teeth to prevention efforts. The company should emphasize its commitment to an austere ethics policy and communicate its stance clearly at every level.

   Both employees and executives should be updated regularly on the impact of current or anticipated abuses and the value they can play in ferreting out fraud. Some businesses have blogs or Web pages dedicated for the purpose of updating employees, business partners, and customers about their efforts and success.

4. Enable enforcement

Enforcement can take the form of both forensic investigations of known or perceived frauds committed, but also regular contract compliance audits of distributors, resellers, external or outsourced service providers and other third-parties.[5]

Perhaps the strongest deterrent to committing warranty service fraud is the fear of capture, prosecution, and retribution. We recommend an active program to investigate and prosecute frauds, with great care taken to inform the public on those efforts and resolutions, just as Nortel did in 2007 when it won a much-publicized $10 million judgment against two businesses participating in a long-running service abuse scam[6].

5. Implement controls to reduce vulnerabilities and limit implications

Fraud perpetrators have grown increasingly savvy in capitalizing on loopholes and other control weaknesses in the product sale to service life cycle. Companies that effectively apply a portfolio of controls that prevent and detect service abuses will be better positioned to reduce fraud and deter future exploitation. Furthermore, we believe that monitoring techniques can be one of the most cost-effective and non-invasive controls available, and have added a separate step to the framework for those efforts.

Serial numbers

Serial numbers and their use in evaluating the legitimacy of service claims provide the most effective line of defense against entitlement abuse. But serial numbers are effective only if they are tracked, leveraged correctly, and kept private.

Contracting

Contracting also represents an important control in preventing service abuse, in conjunction with communication efforts. Contracts should be realistic and enforceable, but unambiguous in expectations and clear on demands for compliance—with teeth to detect, investigate, and penalize non-compliance.

---

5   Details on enforcement efforts, due to their unique nature and criticality in performing these effectively, are not included in this paper. For additional details, please contact PwC.
6   http://www.reuters.com/article/idUKN0746658620070907

Notable controls to reduce vulnerabilities

Serial numbers

- Products sold, including the subcomponents that comprise them, should have unique serial numbers.

- Manufacturers should maintain records of active combinations of serial numbers.

- Serial number lists or databases should be considered confidential, and protected as such.

- Service contracts should list specific serial numbers of products covered under each contract.

Contracting

- Institute a rigorous certification process for third-party service providers that will ultimately incur costs and potential liabilities on the company's behalf.

Sales

- Confirm that service plans and other entitlements are linked to serial numbers for individual products.

- Validate serial numbers where possible when selling service contracts.

- Maintain information, where possible, of product serial numbers linked with recipient information for customer-designated sales.

- Use tools available to evaluate the legitimacy or existence of product and service contract recipients (e.g., authentication of valid addresses and company names, and combinations therein).

- Encourage customers to buy service contracts up front.

Claims processing

- Ensure that technical assistance staff has a solid understanding of what entitlement fraud is, how it is perpetrated and controlled, and its implications for the business.

- Develop a built-in inquiry within customer service software to remind business partners to validate service requests by obtaining mandatory information.

- Train and require customer service representatives and service technicians to maintain proper documentation (such as a service log) for each service request.

- Conduct one-to-one matching between serial numbers of claimed products and valid service contracts.

- Develop diagnostic tests or "common answers" listings to remotely test whether the product experiencing difficulties is "defective".

Service delivery

- Prior to performing service, ensure appropriate approvals or system checks are performed, or that authorization has been granted to third-parties.

- Acquire collateral (such as deposits or credit card numbers) prior to shipping replacement products.

- Require additional approval or notification when third-party service providers are anticipating overruns of predefined cost thresholds.

Returns processing

- Make sure that resellers and distributors conduct a mandatory initial check before they incur any product evaluation costs and before they forward RMAs to manufacturers.

- Obtain confirmation when RMAs or returns have been shipped.

- Match the serial numbers of returned products to service request information as soon as they are received.

- Efficiently test returned products for entitlement, functionality, and authenticity.

Software entitlement abuse

- Use system controls that give buyers access only to the modules that hold the software they have paid for.

- Embed registration controls into software to require buyers to register before it is activated.

- Monitor use of these systems, reviewing for suspicious trends and behavior.

Sales

Companies should also periodically review their sales processes, controls, and other requirements to identify susceptibilities to risk of entitlement abuse.

Claims processing

During claims processing, arm your support teams with intelligence on how frauds are committed and tools (serial number and customer databases) to root out and mitigate losses from fraud perpetrators.

Service delivery

Ensure appropriate approvals and system checks are performed prior to delivering service, and acquire collateral prior to shipping replacement products.

Returns processing

Timely and effective inspection of returned products is critical to reducing further risk of losses from entitlement abuse. Consider leveraging resellers along with their relationships and proximity to customers to provide an initial check of legitimacy and actual need for service or replacement requests.

Software entitlement abuse

Companies have also benefited from software access and registration controls over the years to reduce losses from software entitlement abuses.

Reporting

Provide an internal and external reporting vehicle so that customers and employees can report suspected instances of abuse or fraud, and ensure a process for investigating and following up on escalations.

Survey 6: If your company has controls and programs related to service abuse, how would you describe them? (% respondents agreeing)
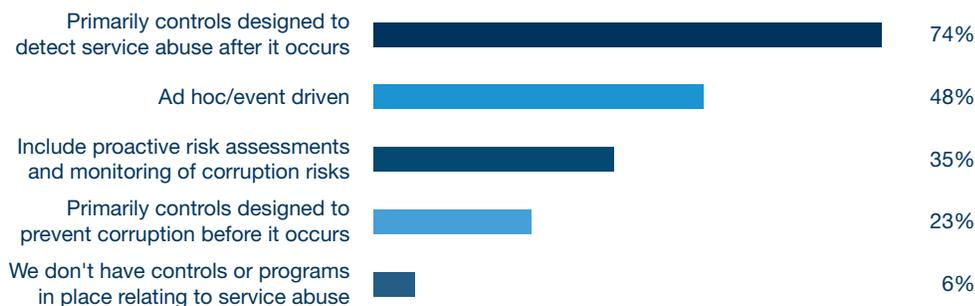
Primarily controls designed to detect service abuse after it occurs	74%
Ad hoc/event driven	48%
Include proactive risk assessments and monitoring of corruption risks	35%
Primarily controls designed to prevent corruption before it occurs	23%
We don't have controls or programs in place relating to service abuse	6%

"Internal Audit can and should play an active role in objectively evaluating and offering solutions to improve a company's controls around entitlement abuse. For example, utilization of continuous monitoring and related audit tools is a trend we see more and more companies benefiting from both an internal audit cost reduction standpoint, but more notably by reducing the instances and implications of warranty service abuse. The return on investment for these controls can be significant."

David Lavoy
PwC Internal Audit
Services Partner

6. Continuous improvement and monitoring mechanisms

Effective monitoring techniques are critical, and should be leveraged to drive continuous improvement and reductions in warranty service abuse.

Techniques are most effective when they are applied in tiers, addressing reactive (tier 1), proactive (tier 2), and predictive (tier 3) elements.

One of the most prominent methods of detecting and preventing entitlement abuses leverages computer-assisted auditing techniques, or "CAATs". Using CAATs, sales, claims, and other data are analyzed regularly for control or policy violations, circumventions, or other red-flags indicative of potential abuses.

Tier 1—Reactive approach

Companies should investigate root causes of fraud schemes and learn from their mistakes or losses. Create a cross functional-team to design and implement methods for strengthening weak points in the manufacturing or claims filing processes.

Tier 2—Proactive approach

Under the proactive approach, the company reviews data or activities for trends indicative of ongoing or potential abuses such as flagging notable transactions; or triggers, such as a service claim for a serial number with notable prior claim activity.

Tier 3—Predictive approach

The most cost-effective monitoring prevents a fraud from ever occurring. Using a predictive approach allows for the identification of trends or precursors to fraud to reduce future abuses. For example:

- Determine the profit margin anticipated from each service contract, then automatically flag customers whose high service use triggers margin short-falls. Then, investigate all related service claims or require additional scrutiny on future claims.

- When a customer buys, for example, 100 products, and only requests service plans on 50, flag the costumer for an additional level of scrutiny, verification, and possible penalties.

> 61% of respondents believe cost is one of the greatest barriers to implementing an effective service abuse program at their company. However, our research indicates a significant return on investment from a prevention program that incorporates the recommendations in this publication.

> Opportunities for mitigation of entitlement abuse-related losses are real and can be inexpensive and non-invasive. Decisions to forego those opportunities should be documented for accountability purposes.

7. Understand and navigate impediments to effective change

Several roadblocks can impede implementation of a prevention program. These may include ingrained and accepted practices that enable abuse, lack of buy-in or change aversion from management and stakeholders, and real or perceived strains on customer relationships.

Accepted industry and business practices

Industry and business practices that facilitate abuse can hamper prevention efforts. Change is particularly difficult to realize when entitlement abuse has become a standard practice across an industry or individual company. Strong management means challenging assumptions and questioning whether the practice is standard because it provides the greatest value to stakeholders, or only because it's familiar and well-established.

Change aversion and lack of stakeholder buy-in

Lack of buy-in from key individuals within the organization can also be an impediment, particularly in a customer-facing business process. Business leaders need to guard against a "that's the way we've always done it" mentality.

Customer service implications

The reluctance to drive change is in part a customer service question. Consumers accustomed to accessing service without providing serial number verification, for example, may resent requests for additional documentation and view them as added and unnecessary scrutiny. Still, business leaders should engage customers and other business partners in a candid conversation, pointing out that the controls are not overly burdensome, and as our research suggests, customers likely will benefit as the costs and magnitude of the warranty service abuses subside.

As Joe Novak, Vice President, Technical Services of Cisco Systems, Inc. said, "You can't run your service abuse prevention program solely out of the back office. You simply must engage the sales team; that means talking to the customers."

The bottom line

Service abuse impacts business through lost revenues and increased costs, and contributes to the gray market, undermining the integrity of both individual businesses and entire industries. These consequences, along with other risks, will continue to threaten a company's operations and financial results unless threats are recognized and appropriate actions are taken to prevent continued fraud and abuse.

Sound risk management strategies can thwart abuse, improve the bottom line, and protect a company's brand. It's time to sweep the money off of the table and put it back into operational performance.

How PwC can help

- Assistance in the development of a warranty service abuse prevention program

- Benchmarking your company's efforts and results against leading practices

- Provide outsource/co-source services to assist clients with their compliance or prevention activities, such as

    — Contract compliance reviews of business partners

    — Development of monitoring tools and strategies

    — Review and resolution of red-flags arising from monitoring efforts

    — Investigations of business partners or alleged fraud perpetrators

About PricewaterhouseCoopers LLP

PricewaterhouseCoopers (PwC) provides industry-focused assurance, tax and advisory services to build public trust and enhance value for its clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

Our Technology Practice provides industry-focused assurance, tax and advisory services for public and private clients. We invest significant resources in building and sharing our industry knowledge, and as a result, we have the scope, depth and expertise to advise technology companies on the changes they face.

Our Licensing Management & Contract Compliance practice guides companies related to licensing management, contract compliance and revenue recovery. We analyze compliance with licenses and other business agreements to help companies realize incremental revenue and mitigate risk.

Our Internal Audit practice provides a range of services, from internal audit outsourcing and co-sourcing, to ERM assistance and Sarbanes-Oxley services, that go beyond traditional financial reporting to help internal audit realize its full strategic potential. PwC's Internal Audit services methodology stresses industry focused, cost effective and value-focused solutions for business transformation.

About AGMA®

The Alliance for Gray Market and Counterfeit Abatement (AGMA®) is a non profit organization comprised of leading high technology companies committed to addressing the global impact of intellectual property rights issues; such as gray market fraud, parallel imports, counterfeiting, software piracy, and service abuse of technology products around the globe. The organization's goals are to protect intellectual property and authorized distribution channels, improve customer satisfaction, and preserve brand integrity. AGMA® uses a variety of avenues to cultivate change in the marketplace including, event speaking, educational initiatives, benchmark studies, industry guidelines, and, where appropriate, public policy advocacy. To learn more about AGMA®'s initiatives or to become a member, please visit http://www.agmaglobal.org/ or contact:

Marla Briscoe
Vice President and Public Relations
Chairperson
(281) 518-7818
vicepresident@agmaglobal.org

Joanne Cooke
Executive Director
(510) 400-8747
jcooke@agmaglobal.org

About this collaboration:

PwC coordinated with AGMA® and its member base, along with other technology companies, in conducting surveys (33 respondents from 14 companies with total annual revenues in excess of $315 billion) and interviews (20 interviews with executives from 10 companies) covering the topic of warranty service abuse. Those efforts, coupled with additional research, served as a basis for the results summarized throughout this paper.

To have a deeper conversation
about how this subject may affect
your business, please contact:

Jonathan Kurtz
Director—Internal Audit and
Contract Compliance Services
PricewaterhouseCoopers
(954) 712-4438
jonathan.kurtz@us.pwc.com

David Marston
Partner, US Leader—Licensing
Management & Contract
Compliance Practice
PricewaterhouseCoopers
(415) 498-6585
david.l.marston@us.pwc.com