Don’t Bet Your Business on a Grey Market Solution
In my role as the OTRS Group COO, I take great pride in the expertise of our global teams. They have produced 735,000 lines of professionally developed code, keeping OTRS in step with changing business environments and modern security standards. They have implemented thousands of OTRS instances across endless verticals during the past decade. They are an expert team that works tirelessly to make sure our customers receive the maximum possible value from our service management solutions.

Working with experts who deliver high quality solutions saves your business from added expenses, dangerous data loss, security issues and even being locked into aging technologies.

The following stories come directly from real experiences our team has had with companies (names available upon request) who have previously worked with grey market providers: If it resonates with you, contact OTRS Group, the official OTRS product manufacturer, to discuss your situation. We're happy to help.

www.otrs.com
sales@otrs.com
THE COST OF DISAPPEARING DATA  4

AGILITY LOST: GREY MARKET PROVIDERS SLOW YOUR ABILITY TO ADAPT  6

ARE YOU GETTING WHAT YOU PAID FOR?  8

VIOLATING DATA PROTECTION REGULATIONS  10

COST AND VALUE ARE NOT THE SAME  12

THE TRUTH IS BLACK AND WHITE  14
THE COST OF DISAPPEARING DATA

– by Francisco Cruz, GM OTRS Mexico –

Initial savings lead to significant unexpected costs down the road. If your business depends on meeting SLAs, or even just keeping customers happy, lost case histories and ticket times can have serious financial consequences.

When we go to upgrade a customer, their biggest worry is almost always if their data will continue to be available. Particularly if they have strict SLAs, customers want to make sure that they have continuous access to the ticket times and histories.

When businesses have worked with grey market providers, preserving their data isn’t always possible. Grey market providers often do two things:

1. They don’t have enough knowledge of OTRS itself, so they “recreate” existing features, which means making a lot of unnecessary changes and modifications. They get the feature working, but have then significantly changed the system in the process.
2. They create what is practically a completely new “product” in how they’ve modified the tables and the source code.

One recent customer would have lost 86% of their data. They will archive the system now and pay the price of starting over again.

In both cases, it means trouble when we go to upgrade. The migration script runs a check on the tables to see if everything that should be there is there and to check if it’s all working OK.

If the system is in its original state, our developers know what has changed from one version to the next and update the script accordingly to make sure that it takes these changes into account and runs through smoothly. BUT, if the tables have been modified, the script fails completely or it drops tables that were unexpected.
When a table is lost, let’s imagine it’s the customer table that tracks all the details of all of a business’ customers, so too is the data in the table. And, even more than that, all of the functions and processes that rely on that table begin to fail because it’s no longer there for reference. Can you imagine losing access to all of the data about all of your customers?

We once had a workforce management company that had modified their system to the point where upgrade was no longer possible. And, they were stuck. When companies get to this point, they struggle with what to do because, on the one hand, their system is now out-of-date which can leave them vulnerable and without the most up-to-date security patches. On the other hand, they face maintaining the old system as an achieve and then re-paying for a new instance and re-spending to customize it again.

It’s tough for companies, because in the beginning they think they are saving money, maybe on consulting, the system or the support package. Yet, in the end, they often end up spending twice as much.
AGILITY LOST: GREY MARKET PROVIDERS SLOW YOUR ABILITY TO ADAPT

– by Nils Leideck, OTRS Product Manager –

Agility depends on having flexible tools and easy access to data. In today’s world, working with grey market providers minimizes both, keeping businesses stuck in the past.

ag.i.li.ty (noun)
the ability to move quickly and easily

How agile are you if you’re locked into your vendor or outdated technology?

As a product manager, my role is to ensure that our teams are working in an agile manner and that we’re enabling our customers to do the same. Working in an agile way means that you can, for instance, change the way your service desk, sales department or DevOps teams work independently of the tools used and at any time. So, you can change people, but leave the processes and tools the same. Or, you can change the tool, but keep the people in place.

Grey market providers make this difficult.

When you have a lot of custom engineering, you have to go back to the grey market provider to handle any changes. You end up having a full-scale project, complete with extra costs and long timelines. Even when it should be a quick update, you can’t simply request a date and be done with it. You have to build out a project with the grey market provider.
In fact, they disabled some of the security settings.

On top of that, the provider had modified the database in a way that required a vendor login, so even if the customer wanted to, they could not update the system or change to another provider.

This is pretty common, and it prevents companies from choosing other vendors, which also limits agility. If you want to adapt your business for any reason – location requirements, new regulatory requirements, or even simply different service needs – you are forced to either drop the system or start over with a new provider... that's not well aligned with modern agile thinking.

I can see this becoming more and more of a problem over time too. As artificial intelligence, analytics and business intelligence take on even more of a role, businesses will need to be sure that their data is structured in such a way that they can take best advantage of modern tools and processes. This means they need to get updates even more quickly. And, if you're stuck with a grey market provider, it's unlikely that you will be able to do so.

Now you are talking about using typical waterfall methods. The simple nature of how you work with a grey market provider limits the ability for a company to work in an agile way.

Additionally, I recently worked with a customer who had purchased specific modules from a grey market provider. The modules were labeled as “OTRS-verified,” but were not at all.
ARE YOU GETTING WHAT YOU PAID FOR?

– by John Coggins, Business Relationship Manager –

What do you do when you have been told you’re receiving one product and have actually been given something entirely different? In this case, the user had to start over completely.

I’ve been with OTRS Group for over six years in various roles as part of our support team. Through these years, I’ve seen all sorts of issues that leave customers in difficult positions after they’ve worked with grey market providers. Sometimes the table structure and database are changed, so tables no longer fit into the OTRS schema. These customers can’t get critical security updates or access to new features during upgrades.

Sometimes grey market providers offer to update ((OTRS)) Community Edition users to the newest version for a reduced price, but then get stuck and can’t continue. Users are without direct support and can’t restore. Can you imagine losing all the history, reports and automation your business has come to rely on?
In 2017, NotPetya ran rampant through multiple major corporations worldwide as it exploited a known vulnerability on unpatched machines around the world. It literally halted operations of the fifth largest shipping company in the world. Estimated total cost was over USD 10 billion.

Right now, I’m working with a customer who contacted OTRS Group because they were having difficulty getting their service provider to answer basic support questions. The customer didn’t have access to the admin tools; and basic tasks, like password resets, would take the grey market provider up to 14 days to address. Anything beyond that would often take in the range of 21 days, and even then, there were situations where the provider simply wasn’t able to offer support.

So, they reached out to OTRS Group as the product manufacturer to see what solutions we could offer. Upon looking at their system, we quickly realized that what the customer believed to be OTRS 7 was actually OTRS 6.0.3. The grey market provider had faked the release files. They had created a skin that mimicked OTRS 7, but the actual system was not what the customer had paid for: It was significantly scaled down and lacked so many of the features and functionality of OTRS 7.

Obviously, this leaves the customer in a difficult position. He’s sold the system internally as one thing and now doesn’t have the functionality they were expecting. They still need a service management solution, but what they have can’t be updated. They face starting completely over without even being able to keep part of the existing data that was generated with the fake OTRS 7.
VIOLATING DATA PROTECTION REGULATIONS

– by Matheus Baeta, Managing Director, OTRS Brazil –

Broken architecture, unreviewed code changes, incompatible security updates… grey market providers can lack expertise that’s necessary to keep your customer data safe.

<table>
<thead>
<tr>
<th>Data Regulation Examples</th>
<th>Where</th>
<th>Possible Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>European Union</td>
<td>EUR 20 million or 4% worldwide annual revenue</td>
</tr>
<tr>
<td>CCPA</td>
<td>California, USA</td>
<td>USD 7,500 per offense</td>
</tr>
<tr>
<td>LGPD</td>
<td>Brazil</td>
<td>2% of turnover in Brazil up to BRL 50 million</td>
</tr>
<tr>
<td>PDPA</td>
<td>Singapore</td>
<td>Up to SGD 1 million</td>
</tr>
</tbody>
</table>

Worldwide data protection regulations are of increasing concern for businesses. Kicked off by the General Data Protection Regulation (GDPR), the world began to look even more closely at how businesses are handling data: fines are now being imposed when businesses demonstrate carelessness. Take for example the recent cases of British Airways being **fined GBP 183 million** by the Information Commissioner’s Office in the EU; Equifax **settling for up to USD 700 million** with the Federal Trade Commission and others in the US; and Integrated Health Information Systems in Singapore being **fined SGD 700,000**.
It’s only a matter of time before the over 120 countries who have data protection legislation in place begin more stringently enforcing these: After all, it’s a revenue stream.

Out-of-date software is a huge vulnerability for businesses when it comes to keeping their data safe. Just think back to the WannaCry and Petya attacks in 2017. Their ability to infect more than 300,000 systems across 150 countries was a direct result of outdated software being used.

And, that’s what oftentimes happens with grey market providers. Customer systems get out-of-date because the cobbled-together grey market systems have broken the underlying OTRS architecture to the point where necessary updates aren’t possible. Businesses and their customer data are left open to attack.

Sometimes too, businesses end up exposed because of unreviewed code changes being made – whether because of nefarious intentions or simply lack of proper expertise. In fact, I have a case right now. When we reviewed the customer’s system, we discovered a substantial number of code changes which have permanently and purposefully locked said system to an older legacy version, without any security updates since 2017.

Why does this matter? Since 2017, there have been 15 security vulnerabilities for which patches were released in OTRS.

Companies that don’t properly apply patches are in danger: In fact, more than half of all reported data breaches are as a result of unpatched vulnerabilities and some of these can cripple an organization.

For instance, most recently, Borontok ransomware has been attacking Linux systems (including files, registry, programs and settings), forcing companies to pay USD 75,000 (in Bitcoin) or have their files deleted within three days. Cayosin is an example of a evolving botnet that exploits multiple vulnerabilities, resulting most often in distributed denial of service (DDoS) attacks. Businesses who have applied the correct patches are safer, but those who haven’t remain at risk.

A team mate is working with another business. Examining that system showed that it had a serious number of web services running and was continuously transmitting data to the grey market provider’s unsecured servers. The customer had no idea; and, of course, the customer is ultimately responsible for the data.

If you aren’t using official solutions, you simply do not know if someone is actually getting access to your customer data who shouldn’t be. That leaves businesses wide open to potential regulatory fines.
COST AND VALUE ARE NOT THE SAME

– by Udo Kampelmann, Managing Director, OTRS Asia –

Getting hooked in by a low initial price point can result in expensive rework and inefficiencies down the road.

Most leaders that I work with are stringently bottom line focused when it comes to their projects. They want today’s technology at the lowest possible price, and grey market providers are willing to offer quick cheap code to accomplish this. Grey market providers employ a business model that is focused on making easy money instead of on long-term reliability, trustworthiness and business relationships.

Once businesses leap to the grey market, they are locked in. They are now dependent upon hacked together software to support their business model. If any changes or modifications to the code are needed, it would be effort-intense to have a developer dig into the hack, understand the logic behind it and adopt it to the new demands of the customer. Or if there is an issue with the software, rendering it unusable, business might even come to a halt.

It is understandable that businesses are looking for the best price, but value needs to be viewed in different ways.

Working directly with the product manufacturer typically pays off within a single year. In only 12 months, you gain the ability to drive long-term sustainable value for your customers.

Real disruptors, those who will lead the technology industry into the future — who will take advantage of AI, big data and cloud options to create novel customer experiences — these people understand that it’s necessary for a company to consistently improve its business outcomes through digitalization.

They know that they must focus on improving efficiencies, increasing retention, reducing costs and upselling customers if they want to stay ahead. Every one of these outcomes will require ongoing and endless optimization to their technology solutions if they work with a grey market provider because these grey market providers only meet an instantaneous need: They don’t develop flexible long-term solutions. So, that system you saved a bit of money on today, is going to need long-term on-going investment to keep pace with changing customer demands over time.
Unlike grey market providers, product manufacturers take a far more holistic approach to development. They have their pulse on the future, evaluating which trends will last to enhance the product long-term and keep customers safe. They know how to pair existing customization options with existing features to get the most value for customers right now. Their financial security and business stability can be trusted. They have access and insight gained from working with industry leaders, like the Federal CERT community in Germany.

At least in the case of OTRS, your long-term business outcomes become part of the solution. This is even true if you need a new feature or process: Each tweak to your instance is done based on best practices so that they don’t need to be reworked and repaid for with every new update. In fact, many times, implementation costs are even partly shouldered by OTRS Group.

The tangible business outcome of picking the product manufacturer over a grey market provider is that your solution can flex far more easily to future process changes that will be necessary for improving efficiency, increasing retention and upselling customers. And, long-term, it does so at a more reasonable cost.

**Cheaper isn’t always better.** And, it isn’t even always the best option for your bottom line.
THE TRUTH IS BLACK AND WHITE

The term “grey market” stems from the fact that providers are selling a solution outside of legitimate distribution channels. The providers work in a grey area — often falling somewhere between the truth and illegality.

The aftermath of dealing with grey market systems is not unique to OTRS Group. But, as both the official product manufacturer of OTRS and as a business that frequently encounters businesses struggling post-grey market encounter, we want to help keep you (and your customers) safe and financially sound — both today and in the long-term.

If we can be of help as you explore service management solutions for your business, or help you investigate a potential grey market developed OTRS instance, contact sales@otrs.com.

Regional office contact information is available corporate.otrs.com/company/offices/.

Use the following checklist when you begin a relationship with any new technology provider:
Step 1. Question licensing and distribution.
Understand how the provider gained access to the software, what rights they have and how this extends to you and your business.

☐ What are the details of your relationship with the official product manufacturer?

☐ Can you provide a written statement authorizing you to resell the product? Do you have rights to use the most recent version of the product?

☐ In addition to the distribution rights, what type of support arrangement do you have with the product manufacturer?

☐ What warranty do you offer? Am I entitled to any manufacturer warrantees?

Step 2. Examine security measures.
Ensure that all necessary steps are being taken to protect your business operations and customer data.

☐ Are your data centers ISO 27001 certified?

☐ What measures are in place to limit physical access to our data?

☐ How are you encrypting data?

☐ How will we know what data is being transmitted to your servers?

☐ What backup procedures are in place?

☐ Are your processes aligned with GDPR (or other applicable data regulations)? If our customer requests data erasure, what guarantees do we have that you will follow through on this?

☐ If our relationship were to terminate, what would happen to my data?

☐ What repercussions do I have in the event of a breach?

☐ What processes are in place to keep my system up-to-date? When and how are patches managed?

Step 3. Evaluate training and expertise.
Determine if the provider has sufficient expertise in working with the software and gain insight into their support methods.

☐ Are you certified with respect to this tool/product/solution?

☐ For how long have you been in business?

☐ Can you offer references from customers who have previously upgraded this system while working under your guidance?

☐ How many installations/upgrades/projects have you worked on specifically with this product?

☐ What is the most complicated configuration you’ve handled?

☐ Ask for reference implementation and interview these customers if possible without the involvement of your supplier.

Step 4. Ask questions about business sustainability.
Double check that this will be a partner who can continue providing on-going support as your business grows. Don’t get stuck with their customized solution and no way to get help should the provider go out of business.

☐ What are your long-term business objectives? Will you be in business when we need help down the road?

☐ What level of access will I have to administrative tools?

☐ What SLAs can we expect? If these are not met, what recourse do we have?

☐ If our relationship were to terminate, what issues would I face when seeking a new consultant/support team?

☐ What issues will I encounter if I want to integrate other tools?