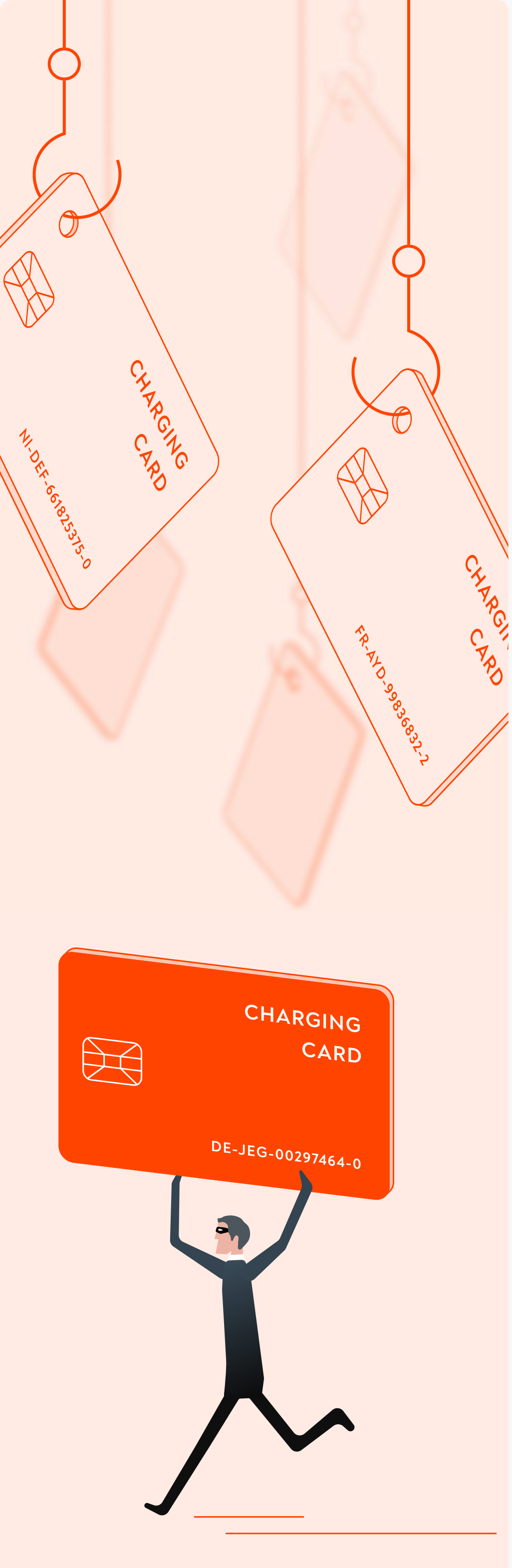
DEFTPOWER

EV charging fraud

How to prevent EV charging fraud: A guide for MSPs and fleet operators



Unpaid invoices, cloned charging cards, and inflated reimbursement claims can quickly add up for charging providers, especially when fraud stays invisible. Here is how MSPs and fleet operators can detect fraud earlier and reduce cost leakage before they appear on the invoice.

For Mobility Service Providers (MSPs) and fleet operators, EV charging fraud is difficult to control because it often looks like normal charging activity until the cost has already been created. A payment method passes onboarding. A cloned charging card produces valid-looking sessions. An inflated reimbursement claim looks reasonable enough to approve.

The level of fraud risk depends on how a charging service is set up. Open registration, delayed billing, RFID cards, virtual tokens, and manual reimbursement each create different points where misuse can enter the flow. That is why fraud prevention cannot rely on one generic measure. It requires a combination of controls that match the specific risk.

Deftpower helps MSPs and fleet operators catch errors, fraud, and misuse before they turn into losses, with controls placed at every stage of the charging process, from before a session starts to after it ends. This white paper walks through where those points are and how each control lever works.

What is EV charging fraud?

EV charging fraud is any deliberate act of deception or misrepresentation used to obtain charging services, claim reimbursement, or shift costs to the MSP without legitimate right. It covers three categories:

01

Payment fraud: charging starts before payment risk is properly controlled, and the MSP cannot collect afterwards.

02

Token fraud: a charging card or virtual token is cloned, shared, or used in a way that does not match the registered driver, vehicle, or policy.

03

Reimbursement fraud: a driver claims a higher home electricity tariff than they actually pay, and pockets the difference.

01

Payment fraud: failed payments and unpaid invoices

Payment fraud happens when charging starts before payment risk is properly controlled. In open-registration B2C charging services, a driver may create an account, add a payment method that passes a basic e-mandate check, and start charging. When the MSP tries to collect payment later, the payment fails. The account can be blocked, but the energy has already been delivered.

This risk increases when drivers use limited-credit virtual cards, false contact details, or payment methods that can be blocked after the session. Every failed collection becomes a cost the MSP may not recover.

For invoiced B2B and fleet accounts, the risk is slightly different. The customer may be legitimate, but charging can continue while unpaid balances, overdue invoices, or credit exposure grow. That is not always fraud in the strict sense, but it creates the same commercial problem: the MSP carries the cost before payment is secured.

How Deftpower prevents payment fraud

Deftpower reduces unpaid invoice risk with two controls: pre-authorisation and credit limits.

Pre-authorisation is most relevant for open-registration B2C charging services. Before the charging session begins, Deftpower reserves an amount on the driver's payment method through the payment service provider integration. If the reservation fails, the session does not start.

Pre-authorisation stops high-risk sessions before energy is delivered and the cost becomes an unpaid invoice. In two recent cases, providers running pre-authorisation saw unpaid invoice ratios drop from over 15% down to around 1% in the first full quarter after activation.

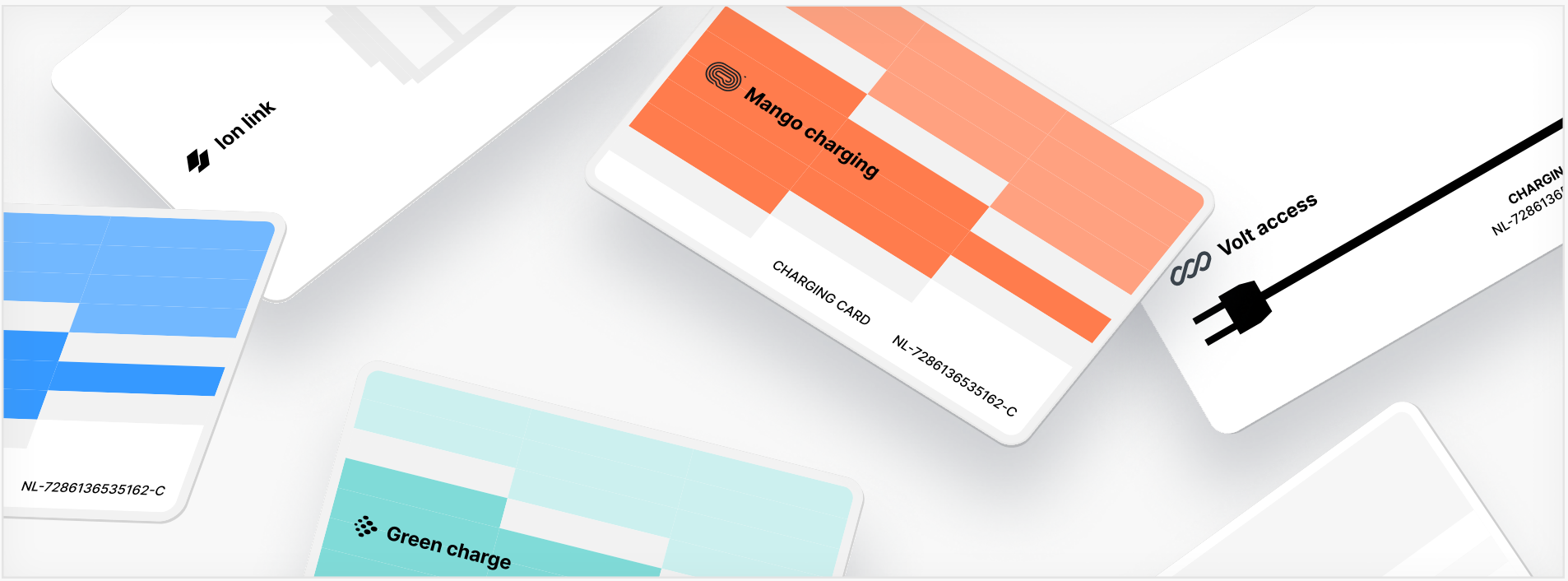
Credit limits add protection for invoiced accounts and fleet customers. MSPs can set limits on the unpaid balance, the number of unpaid invoices, or the number of days an invoice remains overdue. When those thresholds are exceeded, charging cards can be blocked automatically until the account falls back within the configured limit. Credit limits can be applied flexibly, with separate thresholds for higher-risk segments without affecting trusted accounts.

Over 80% of credit limit blocks are resolved once the driver pays the outstanding balance. They're usually customers who missed a bill and settle up when the token is blocked. The rest stay blocked, so no further costs can build up on the account.

These controls help MSPs manage both sides of unpaid invoice risk: failed-payment fraud before charging starts, and open credit exposure before unpaid balances grow too far. Detection rules can be configured for specific use cases. A leasing company managing corporate fleets needs different thresholds than a direct-to-consumer charging service.

02

Token fraud: cloned or misused charging cards



Token fraud happens when a charging card or virtual token is copied, shared, or used in a way that does not match the registered driver, vehicle, or policy. That can happen in several ways:

- A charging card is cloned or copied and used by someone else.
- A valid card is shared or used outside policy, for example to charge another vehicle.
- A token remains active when it should have been blocked or reassigned.

Why charging cards are easy to clone

Most physical charging cards rely on the MIFARE Classic RFID standard, which is not encrypted. The identifier on the card can be read and copied with widely available hardware, including a standard smartphone with an RFID reader. Some MSPs even print the card identifier on the card itself, which means a photo of the card can be enough to start charging on someone else's account.

Plug & Charge (ISO 15118) addresses this at the protocol level by tying authentication to a certificate inside the vehicle itself, which cannot easily be copied. It is the most secure form of authentication available today, but adoption is still limited because it requires three-way compatibility between the CPO, the vehicle, and the MSP. Until Plug & Charge is broadly supported, behavioural detection is what protects MSPs from cloned and misused tokens.

Why token fraud is hard to spot

For MSPs and fleet operators, token misuse is difficult to detect because the sessions often look legitimate. They are linked to a known token, a real charging point, and a completed CDR. But a valid token does not prove that the right driver, vehicle, or use case was behind the session.

This is especially costly in fleet charging. If the driver does not pay the bill directly, misuse can blend into normal charging behaviour. A fleet may assume the driver drove more, charged more often, or used more expensive locations, while the extra cost keeps adding up.

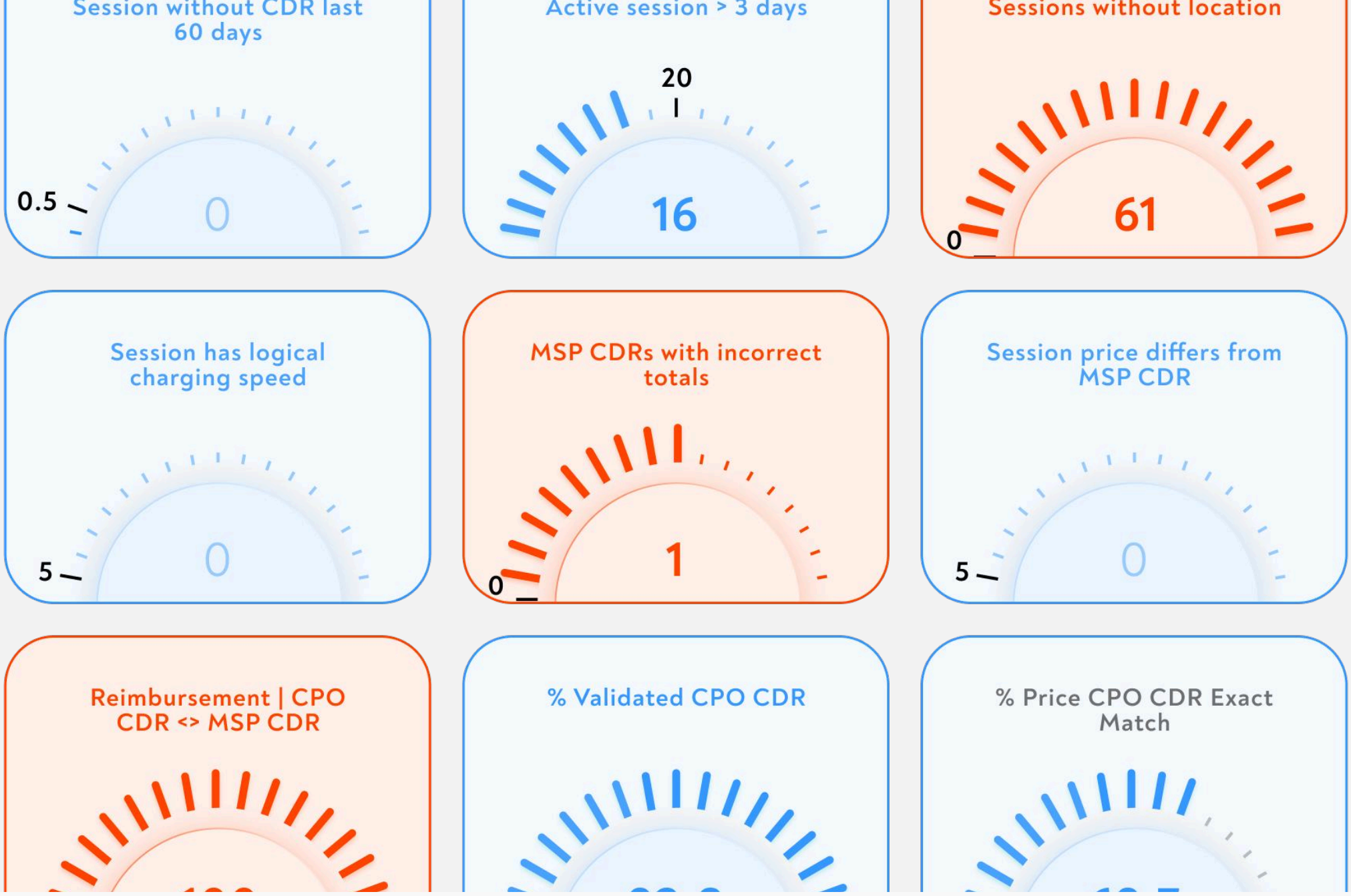
How Deftpower detects token fraud

Deftpower runs continuous fraud checks on all sessions within a look-back time-window. The system looks for concurrent sessions on the same token, unrealistic travel distances between charging locations, excessive energy consumption, and first-time use of newly activated tokens. Together these signals flag sessions where the token may be misused, even when each individual session looks legitimate.

When fraud is suspected, the administrator receives an alert and decides how to respond based on the account's configuration.
When fraud is confirmed, Deftpower blocks the token and both the admin and the driver are informed.

Every blocked or flagged session returns a specific reason, so providers can resolve disputes, support tickets, and audits without any guesswork.

Confirmed fraud blocks rarely get resolved. Around 70% stay blocked permanently, since the accounts behind them were never legitimate to begin with.



03

Reimbursement fraud: inflated home reimbursement claims

Reimbursement fraud is most relevant for fleet charging, where employees are reimbursed for home charging costs. It happens when a driver submits a higher home electricity tariff than they actually pay. For example, a driver paying €0.25/kWh at home might submit €0.45/kWh and keep the difference.

This is difficult to detect because the claim can still look reasonable. A tariff may fall within a plausible range, but that does not mean it reflects the driver's actual energy contract. At fleet scale, manually checking every tariff against market rates or contract data is not realistic, so small differences can add up over time.

How Deftpower validates reimbursement claims

Deftpower validates submitted home charging tariffs against local energy market data. Claims within a reasonable range move through without manual review. Outliers are flagged for review.

This helps fleet operators and MSPs identify inflated or unusual tariffs before reimbursement is approved, while keeping the process smooth for honest drivers.

How your platform setup affects fraud risk

The fraud risk an MSP carries is shaped by a handful of setup choices. Reviewing where your platform sits on each dimension is a useful starting point for understanding your exposure:

01

Payment method. Unsecured payment methods (invoice, unverified direct debit) carry the highest fraud risk in B2C. E-mandates with pre-authorisation reduce that risk significantly.

02

Authentication method. RFID charging cards are the most common and the most clonable. Virtual tokens are convenient but require strong behavioural monitoring. Plug & Charge is the most secure but is not yet widely supported.

03

Billing cycle. Monthly billing means failed payments are only detected at the end of the cycle. Session-based billing surfaces issues immediately but increases PSP transaction fees.

04

Reimbursement model. Manual home charging reimbursement without tariff validation creates an open door for inflated claims at fleet scale.

05

Onboarding controls. Whether you check email domains, verify addresses, and validate payment methods at registration determines how much risk enters the platform in the first place.

There is no single right answer for any of these. The right setup depends on your audience, your risk appetite, and the trade-off you want to make between user experience and exposure. What matters is that each choice is made deliberately, with the right detection layer behind it.

Vehicle data: the next level of validation

Charging cards, payment methods, and CDRs give MSPs important signals, but they do not always prove that the right vehicle received the energy. As more drivers connect their vehicles through the MSP app, vehicle data can add another layer of validation.

01

Odometer readings can help confirm whether energy consumption realistically corresponds with mileage.

02

State of charge before and after a session can help validate whether the energy recorded in the CDR matches what entered the battery.

03

State of vehicle through active power (kW) readings can confirm whether the registered vehicle is actually charging during a session. A zero reading during an active session is a strong signal the card is being used on a different vehicle.

04

Vehicle location can confirm whether a vehicle is actually present at the charging station when the session is taking place.

This makes fraud harder to hide. A token can be copied, shared, or misused. Vehicle data helps confirm whether the energy is actually being used by the registered driver and vehicle.

Deftpower is building this into its billing and fraud detection layers, using vehicle telemetry to strengthen validation beyond the token itself.

Visibility is how MSPs catch misuse early

Not every anomaly is fraud—but every anomaly deserves investigation.
A cloned card produces a session identical to a legitimate one, using the same token, charging point, and CDR. A virtual credit card passes the initial payment check. An inflated home tariff remains within the plausible range. Each looks like normal charging until the money is already gone.

Across the industry, MSPs use a patchwork of solutions to manage back-office billing, roaming networks, and payment providers, each opening the potential for fraud to seep in, since these systems don't share data. Monthly billing cycles compound the delay: a bad actor gets four weeks of charging before the first payment attempt, and by the time it fails, the MSP will have losses to absorb.

Deftpower offers MSPs a white-label charging platform with full visibility into every charging session, across public charging and home charging, and across the driver side and the CPO side of the transaction. Fraud prevention runs continuously in the background, flagging misuse early and automatically blocking tokens or stopping sessions when fraud is confirmed.

Providers running these controls have seen unpaid invoice ratios fall from over 15% to close to zero within 3 months since activation. Deftpower acts decisively to block fraudulent accounts permanently while credit controls resolve as the accounts settle.

Curious how much fraud and misuse is currently going unnoticed on your platform? Get in touch with our team for a closer look.

FAQ

Q **What is EV charging fraud?**

A EV charging fraud is any activity that creates charging costs an MSP or fleet operator cannot legitimately recover, or that inflates costs beyond what was actually consumed. It covers three categories: payment fraud, token fraud, and reimbursement fraud.

Q **Can RFID charging cards be cloned?**

A Yes. Most charging cards use the MIFARE Classic standard, which is not encrypted. The card identifier can be read and copied with widely available hardware, including a smartphone with an RFID reader. Behavioural monitoring is the most practical defence until Plug & Charge is more widely supported.

Q **How can MSPs detect cloned or misused tokens?**

A By analysing charging sessions for patterns that cannot reasonably match the registered driver or vehicle, such as concurrent sessions on the same token, impossible travel distances between sessions, or excessive energy consumption.

Q **What is pre-authorisation in EV charging?**

A Pre-authorisation is the practice of reserving an amount on a driver's payment method through the payment service provider before a charging session begins. If the reservation fails, the session does not start. This stops high-risk sessions before energy is delivered and unpaid invoices are created.

Q **How can fleet operators prevent inflated home charging reimbursement claims?**

A By validating submitted home tariffs against local energy market data. Claims within a reasonable range can be approved automatically. Outliers are flagged for review before reimbursement is paid.

Q **What is Plug & Charge and why is it more secure?**

A Plug & Charge (ISO 15118) is an authentication standard that uses a certificate stored in the vehicle to authenticate the driver and start the charging session automatically. Because the certificate cannot easily be copied or falsified, Plug & Charge is more secure than RFID-based authentication. Adoption is still limited because it requires compatibility between the CPO, the vehicle, and the MSP.

Q **How can vehicle data help prevent EV charging fraud?**

A Vehicle data such as odometer readings, state of charge, and active power can confirm that the energy recorded in a CDR matches what actually entered the registered vehicle. Tokens can be cloned and tariffs can be inflated, but vehicle data ties the session to a specific car, which is much harder to fake.

W www.deftpower.com

E info@deftpower.com