Risk & fraud management with carrier billing

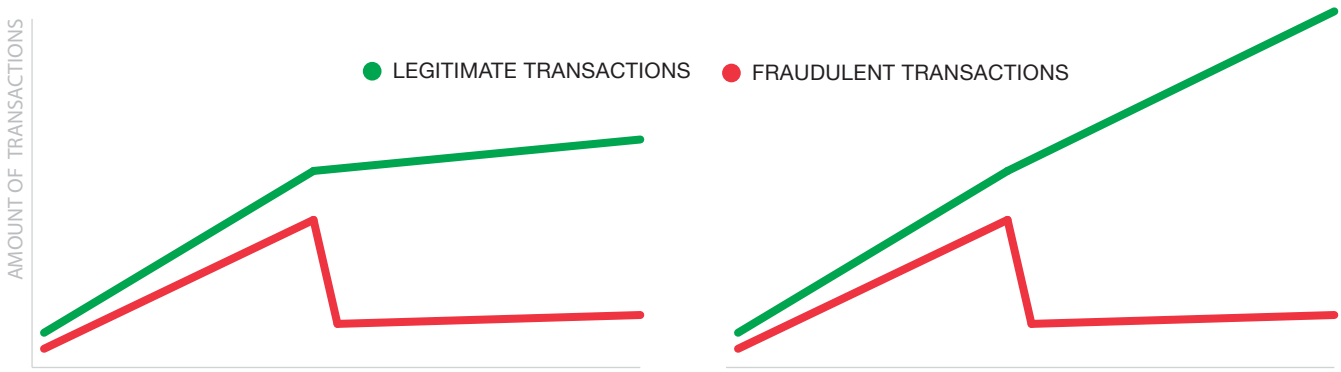
White paper by Fortumo

Introduction

This white paper gives an overview of how fraud and risk management should be implemented for carrier billing. The topics covered in the white paper are:

- Types of fraud and their likelihood with carrier billing
- Attributes that can be used for assessing user and transaction risk with carrier billing
- Mitigating risk through applying (dynamic) spend limits to user groups
- Criteria that should be considered when accepting and rejecting transactions
- Examples of dynamically managing spend limits and assessing transactions
- Suggestions for merchants in order to reduce their fraud risk with carrier billing

When revenue from any payment method for a merchant grows, the merchant tends to become a more attractive target for fraudsters who attempt to exploit their service as well as "friendly" fraud (increase in chargeback requests from users). Usually this results in the introduction of fraud prevention solutions which often are too harsh. As a result, while fraud will be prevented, the amount of legitimate transactions and users that will be rejected grows as well:



Fraud rules configured to be too strict.

Properly configured fraud rules.

Proper risk management processes and solutions allow merchants and mobile operators to increase revenue (enabling higher spend limits and allowing transactions from top spenders) while minimizing damage (reduced amount of fraudulent payments and users).

It is important to note that this white paper will mainly focus on risk management and not fraud prevention. The reason is fraud is significantly more complicated with carrier billing than with card-based payments, as will be described later in the white paper. The focus of risk management with carrier billing is on bad debt, avoidance of "bill shock" and enabling legitimate users to make as many purchases as they want while cutting off risky users.

What types of fraud can occur with carrier billing?

With card-based payments, phishing and card information theft are the most common causes of online fraud. With carrier billing, using another person's phone account for fraudulent transactions is extremely rare. The reason is that the user always needs physical access to the device (SIM card) which is used to confirm the purchase. This makes situations where someone else other than the SIM card owner attempts to make a purchase unlikely.

Another reason why such fraud is rare with carrier billing is that the payment method is mainly used for digital goods (e.g. items which are non-transferable and can be easily "called back" by the merchant, such as in-game currency or a music subscription). This makes the payment method an unattractive target for fraudsters. But as carrier billing is also being implemented in new segments (ridesharing, ticketing, virtual credit cards and digital wallet top-ups) the likelihood of such fraud will increase in the future.

Based on our experience of providing carrier billing in 10 years, the most common cases of fraud with carrier billing are:

LOW RISK

1) Deceptive activity by a merchant. In this type of fraud, a merchant using carrier billing attempts to: (a) have the consumer make a transaction unknowingly, for example through billing them "silently" without the user understanding it; (b) try to bill the user for a higher amount than they have been displayed at the checkout screen or (c) subscribe a user to a recurring payment flow instead of a one-time purchase.

Fortunately for consumers, this type of fraud has been virtually eliminated from carrier billing. Fortumo and mobile operators have implemented compliance management to review each merchant before their services are launched and a dedicated risk management team reviews merchants on an ongoing basis to make sure they stay compliant. Checkout flows hosted by Fortumo also make it impossible for fraudsters to display incorrect payment information to consumers.

LOW RISK

2) Carrier infrastructure technical issues allowing free purchases. In rare cases, it can happen that a mobile operator does not deduct money from the user's account for a purchase. If this happens, fraudulent users who notice the issue might attempt to make many payments in order to get a service for free. In order to combat this type of fraud, carriers have put in place automated checks on their billing platform to make sure payments are working as they should; Fortumo additionally detects and stops end-user activity of this type based on velocity rules.

LOW RISK

3) Phishing attempts to make another user pay on the fraudster's behalf. The fraudster attempts to have another person make the transaction on their behalf. For example, this fraud might be attempted as follows:

1. The fraudster opens up the payment window and enters a legitimate user's mobile number;
2. The legitimate user receives the PIN on their phone in parallel with the fraudster sending the legitimate user a message, attempting to deceive them into forwarding the PIN code to them;
3. The legitimate user becomes confused and forwards the PIN number to the fraudster;
4. The fraudster enters the PIN number into the checkout window and completes the purchase;

Such type of fraud is the closest to card-not-present phishing fraud where fraudsters attempt to collect data from legitimate users in order to make transactions. However, the likelihood of such a scenario is very low. The reason is that payment confirmation messages include information on what is being attempted to purchase; if the legitimate user receives such a message and has not initiated a transaction on their own, they are unlikely to fall victim to the phishing attempt. Such type of fraud can also be reduced by increasing consumer awareness, both by merchants and mobile operators.

This type of fraud is additionally minimized by the usage of account hopping, velocity and attribute rules established by Fortumo and used to block suspicious transactions.

LOW RISK

4) Stolen phones and SIM cards used are used to make a purchase. Stolen SIM cards are significantly more difficult to use for making transactions than stolen bank cards. 70% of phones are protected by a lock screen password and inserting the SIM into another device will require the fraudster to enter the user's PIN number which they are unlikely to know.

Such fraud is additionally limited by a majority of the world's SIM cards being prepaid (US: 24%, UK: 38%, Brazil: 74%, India: 95%, Indonesia 98% etc.). Such SIM cards are useless to fraudsters as they generally have a low account balance (in India, the average account balance is $0.7) and would require the fraudster themselves to add money to the SIM card in order to make a transaction. The same measures are used as with phishing attempts to prevent fraud in this case: account hopping, velocity and attribute rules.

HIGH RISK

5) Consumer chooses to not pay their phone bill. The previously described fraudulent activities are rare due to being complex to achieve and with little benefit for the fraudster. This means the most common type of fraud with carrier billing is users deciding to make seemingly legitimate purchases but not paying their phone bills.

Such fraud is only possible with postpaid SIM cards as the user has an open limit with the carrier; in case of prepaid SIM cards, the user needs to load additional money to their account before they can make further transactions. Even if the transactions are not fraudulent (e.g. underage people making purchases with their parent's phone), this type of fraud can cause merchants issues with carriers and for carriers with telecommunications authorities.

This means that risk management should be the biggest priority for all parties involved in processing carrier billing transactions. While the previous types of fraud described can be prevented through measuring velocity and attribute criteria, spend limit management plays the most important part in preventing bad debt and a resulting loss in revenue.

What do we know about the customer and how does it help in managing risk?

Risk management with carrier billing is done in collaboration between the three parties involved in billing: the merchant who delivers the service, the payment aggregator (e.g. Fortumo) and the mobile operator who charges the end-user.

Risk evaluation should be done for both each consumer (deciding whether the user is eligible for a purchase and how much they should be able to spend) as well as for each transaction (whether such a transaction is allowed for the specific consumer and whether it is allowed in general).

Criteria which are taken into account for risk management with carrier billing are:

Criteria	How can it be used?	Information source
Subscriber identity (MSISDN, ACR, network provider)	Allows tracking historical credit score and payments across platforms & merchants.	Mobile operator
Account age	Longer duration of contract correlates with lower risk of bad debt.	Mobile operator
Subscriber group (prepaid, postpaid, corporate, promotions)	Prepaid customers are considered less risky for bad debt while postpaid correlate with higher ARPU.	Mobile operator
Provisioning status (spend limit, active barring)	Allows evaluating transaction against carrier-defined risk and whether a transaction should be allowed at all.	Mobile operator
Past record with carrier	Customers who have created bad debt, refunds or complaints in the past are likely to do it again in the future.	Mobile operator
Payment history with other merchants	Purchases and refunds with other merchants allows assessing credit score of user.	Payment service provider (e.g. Fortumo)
IP, cookie, geolocation information	Allows validating whether user is who they claim to be.	Payment service provider (e.g. Fortumo)
User behavior with merchant	Account ID, age, past transactions with other payment methods etc. with merchant, allowing to evaluate the user's credit score with the specific merchant.	Merchant

How to mitigate bad debt risk with spend limits?

As described earlier, bad debt by seemingly legitimate subscribers is the biggest risk to both merchants and carriers. Therefore, it makes sense to limit the users' spending capability to reduce the potential amount of damage that can be done. Before launching carrier billing, carriers should define a list of user segments, assess what the spend limits for these segments should be and whether payments should be allowed for each segment or not.

A basic example analysis of how such categories can be created is as follows:

- Mobile operator ARPU for pre-paid users in their market is $15
- Mobile operator ARPU for post-paid users in their market is $45
- Pre-paid users are considered high-risk in case their account is newer than 1 month
- Pre-paid users are considered low-risk in case their account is older than 1 month and have no negative record with carrier
- Post-paid users are considered high-risk in case the account is newer than 6 months
- Post-paid users are considered low-risk in case the account is older than 6 months and have no negative record with carrier
- Post-paid users are considered very low risk in case of account being older than 12 months, ARPU exceeding average post-paid by 3x and have no negative record with carrier

This simplified example (not taking into account background information from merchant or the payment service providers' data on the whole country, instead relying on information only from the carrier) already provides us sufficient information to categorize users into initial spend limit groups:

- **Pre-paid (high risk, <1 month):** daily spend limit $2, monthly spend limit $30
- **Pre-paid (low risk, >1 month):** daily spend limit $4, monthly spend limit $60
- **Post-paid (high risk, <6 months):** daily spend limit $2, monthly spend limit $30
- **Post-paid (low risk, >6 months):** daily spend limit $4, monthly spend limit $60
- **Post-paid (low risk, >12 months):** daily spend limit $12, monthly spend limit $180
- **Negative record with carrier (bad debt, refund, or complaint):** disable carrier billing

While under this model each user is categorized into a spend limit segment for their first purchase, spend limits should be managed in an automatic way so that for additional transactions, users can be moved between segments. If necessary, blacklisting or whitelisting can be applied to specific users.

For users who have a long-term positive spend behavior, automatic (or user confirmed) adjustments can be made to enable a higher spend limit, described later in the white paper.

How to decide if a transaction should be rejected or not?

Once a user has been categorized for a spend limit, the initial check for a transaction should be done for whether a user is allowed to make the transaction or not: whether they are not blacklisted and whether the transaction would not exceed the spend limit of the user, based on the segment they have been placed in.

Additional checks are performed based on established payment behavior ("velocity rules") as well as criteria validating whether the user is who they claim to be ("attribute rules").

Once the initial decision ("User is not barred from making payments and the transaction does not exceed their spend limit") has been made, the following rules should be checked for whether the transaction should be accepted or rejected:

Velocity rules:

- **Transaction frequency.** When did the user make their last purchase and how does it compare to the average purchase frequency? What is the minimum amount of frequency allowed between two transactions? Example rule: Frequency of transactions by one unique MSISDN must be more than 30 seconds apart.

- **Spend limit.** What is the amount of money a user can spend during a specific timeframe? In addition to monthly and daily spend limits, should a user be barred from making payments when they start reaching the monthly spend limit too quickly? Example rule: If a MSISDN reaches 80% of monthly spend limit in less than 14 days into the month, the transaction must be rejected.

- **Bad debt likelihood.** Based on past statistics, if a user from this user category makes a transaction of this size, how high is the likelihood of a future refund, complaint or bad debt? Example rule: If over 10% of users who have made a transaction of this size in the past have filed a complaint, created bad debt or requested a refund with the carrier, the transaction must be rejected.

- **Merchant average.** How much money do average users in this group spend with the merchant? Does this transaction fall into acceptable range of the merchant? Example rule: If an MSISDN is used to make a payment that would exceed the average transaction size of the merchant from this user category by more than 30%, the transaction must be rejected.

Attribute rules:

- **Account hopping.** An average user will have one account with the merchant they are making payments for. Therefore an MSISDN being used to make purchases on multiple accounts with the same merchant are likely be fraudulent. Example rule: If a unique MSISDN is associated with two user IDs within 30 days, the transaction must be rejected.

- **MSISDN hopping.** An average user will have one SIM card to make purchases online. Therefore if several MSISDNs are used for transactions with account of the merchant to make payments, the payments are likely to be fraudulent. Example rule: If a user ID uses more than 2 MSISDNs within 30 days to make transactions, the transaction must be rejected[1].

[1] In markets such as India, people generally use several SIM cards (e.g. one for calling and messaging and another one for mobile data). In such markets, this rule should be removed or criteria made significantly higher.

- **Device hopping.** An average user will have a limited amount of devices on which they consume content and pay for it online (e.g. a smartphone, a tablet and a laptop). If a large number of devices are used to make purchases from the same MSISDN, the payments are likely to be fraudulent. Example rule: If more than 5 devices are associated with the same MSISDN within 30 days to make transactions, the transaction must be rejected.

- **Location mismatch.** A majority of people are likely to stay geographically in the same area, for example their hometown. In case their geolocation changes often, the transaction might be considered fraudulent. Example rule: If two transactions from the same MSISDN are done from IPs not located in the same geographic region within 24 hours, the transaction must be rejected.

- **Payment initiation and finalization mismatch.** With carrier billing, transactions are either initiated and completed on the same device (e.g. smartphone) or across two devices (e.g. initiated on a laptop and confirmed on a smartphone). In the second case, if the locations of the two devices do not match, the transaction might be fraudulent. Example rule: If a transaction is initiated on one device and completed on another one, the locations of the two devices need to be located in the same IP range; otherwise reject the transaction.

- **Timing of the transaction.** Most people make payments during evening times (when they are off work) and during weekends. This means that in case a user makes a transaction on a Wednesday at 5AM local time, the transaction could be fraudulent. While this criterion alone is not enough to reject a transaction it can be assessed together with the previously described criteria to determine the legitimacy of the purchase.

- **Cross-merchant referencing.** If the mobile operator or payment service provider has such capability available, the user's past purchase history can be compared against their current transaction. For example, if a user has previously bought stickers in another social network for $2 per month and now attempts to make a transaction for $30 in a new social network, the transaction could be fraudulent. While this criterion alone is not enough to reject a transaction it can be assessed together with the previously described criteria to determine the legitimacy of the purchase.

If the transaction passes all the criteria, the transaction is accepted. Next, we look at whether we should do anything with the user's spend limit and whether we should blacklist or whitelist them.

How to decide if a user's spend limit should be modified?

In case of a transaction being rejected due to a high risk score, the user can either be put on a watch list (for example, by asking them to take additional steps to verify their identity and re-enable payments) or in case of a very high risk score, blacklisted and blocked from future transactions.

But what if a transaction succeeds and the user's next purchase would fail as they would reach their spend limit? Here the decision must be taken among three alternatives:

- In case of high bad debt risk, retain the user's existing spend limit
- In case of medium or low bad debt risk, increase the user's existing spend limit
- Whitelist the user in case they are evaluated to be in a very low risk user segment (should be used sparingly and only for consumers with a very long, positive credit score)

An example calculation of whether to increase a user's spend limit after a successful transaction could be as follows:

- John is a post-paid (low risk, >6 months account) user who spends $50 monthly on carrier billing and $45 on other telco services. His total spend with the carrier is $95 per month
- John's existing spend limit is $4 per day and $60 per month
- John has hit the $60 per month spend limit this month and we need to decide whether to increase his spend limit
- In his existing segment, risk of bad debt of users like John is 1%
- The next spend limit for carrier billing is $100 per month, meaning John would be billed for up to $145 ($45 from other telco services + $100 for carrier billing)
- In the $100-$150 segment, carrier bad debt risk for consumers is 1.5%
- Extrapolating the decision about John to 1000 users, we see that:
    - Bad debt would be $2175 (1000*1.5%*$145)
    - Total revenue would be $142,825 (1000*98.5%*$145)
    - In existing segment, bad debt is $950 (1000*1%*95)
    - Revenue in existing segment is $94,050 (1000*99%*95)
    - As a result of increasing revenue for 1000 users like John, while our bad debt risk grows by 50%, we stand to gain $48775 in revenue (51.8% increase)
- Now let's take a look at increasing the limit again. Say John reached the $100 level and we want to increase his spend limit to $150 with carrier billing. In the $150-$200 segment, carrier bad debt risk for consumers is 15%. In this case, comparing to his existing spend limit:
    - Bad debt would be $29,250 (1000*15%*$195)
    - Total revenue would be $175,500 (1000*90%*$195)
    - In this case, it does not make sense to increase the spend limit. Our bad debt risk grows 15-fold while our revenue grows by only 22%

Example: what happens if a user tries to make a payment?

Below, let's take a look at an end-to-end example of a user who attempts to make a payment with carrier billing, with proper risk management in place by the carrier and merchant.

User story: Customer James attempts to make a first-time purchase, buying a sticker pack worth $2.99 with social network ABC.

Here is how the decision process would look like:

1. James is a postpaid user with a duration of contract over 1 year with no previous bad debt, complaints or refunds with the carrier. Carrier has decided that this is a low risk user and the spend limit will be set to $50 per month and $10 per day. Customer is not blacklisted or whitelisted.

2. James has made two payments over the past 30 days with carrier billing, totaling $15. There are five days left in the monthly spend limit cycle so James is unlikely to reach the spend limit for this month.

3. James has not made any payments in the past 24 hours. Transaction frequency is acceptable.

4. Likelihood of bad debt for James (based on their segment) is 1%. Bad debt risk is acceptable.

5. The average user in James' segment buys a sticker pack worth $4.99 with the merchant; James' purchase is below the average transaction. Merchant-specific user behavior is acceptable.

6. The average transaction size for users in James' country is $3.8. Country-specific user behavior is acceptable.

7. James' MSISDN has not been used for any other accounts with the social network and James' account has not used any other MSISDNs to make transactions. Account or MSISDN hopping not detected.

8. James initiated payment from device with an IP of 1.2.3 and the payment confirmation is being attempted by a device with an IP of 1.2.4. Both devices appear to have the same geolocation.

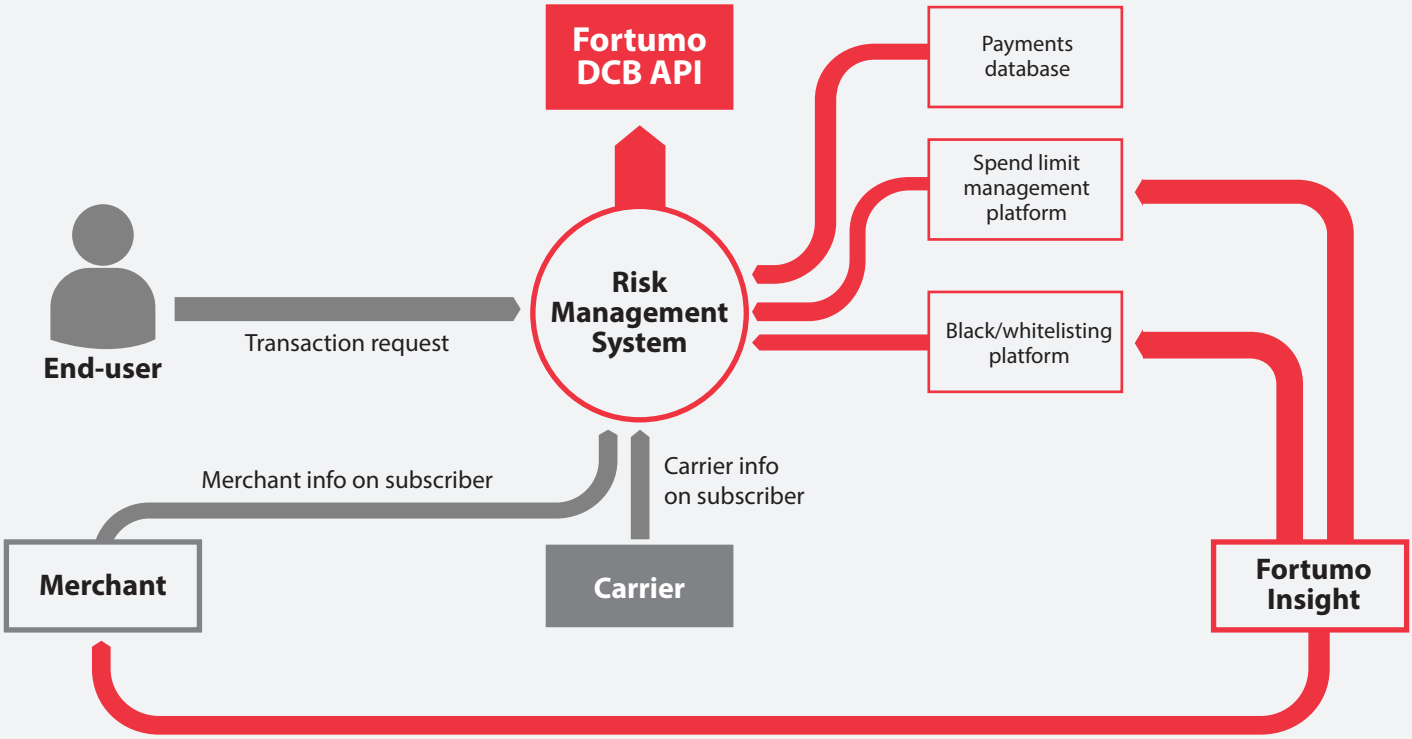
9. James is purchasing the sticker pack at 8PM, the hour with the heaviest payment traffic in the country. Timing of the transaction appears acceptable.

10. Decision: process the payment.

11. James has now spent a total of $17.99 out of their $50 monthly spend limit. As there is a reasonable limit left for James, we do not need to evaluate changing his spend limit.

How does Fortumo help merchants and carriers with risk management?

Fortumo has in place a Risk Management System which assesses transactions and dynamically modifies spending limits based on input from carriers and merchants:



The Risk Management System is maintained and modified by our dedicated risk management team that among other activities, reviews spend limits and modifies attribute criteria and user spend segments.

For carriers, Fortumo has also made available Fortumo Insight through which carriers can monitor and change spending limits for user segments and individual users, as well as manage black- and whitelists.

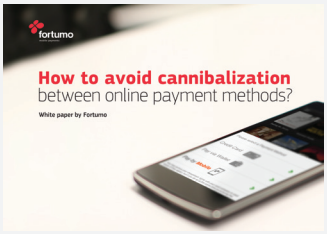
How can merchants mitigate fraud risk with carrier billing?

In addition to Fortumo and mobile operators actively working on risk management, we recommend merchants take the additional steps to mitigate risk:

- Merchants should have on their side a dedicated risk and fraud analysis team in place with capability to monitor and investigate suspicious user behavior; there should also be capability developed to view the user's past purchase history across all payment methods and block specific accounts and MSISDNs from making transactions
- Asking consumers for their mobile phone number on sign-up and authenticating the phone numbers can be used to both increase conversion (pre-fill numbers during the checkout process) while also increasing security
- In case merchants have the user's e-mail available, the merchant can send the user a receipt with each purchase, similar to bank-based transactions (Fortumo and the carriers also confirm the transaction through text messages)
- To mitigate "friendly" fraud (chargebacks), a clear refund policy and the capability to block users with past complaints should be implemented

Additional reading

White paper for mobile operators: keeping up and profiting from the digital ecosystem



White paper: How to avoid cannibalization between online payment methods

Swisscom case study: how do mobile operators benefit from direct carrier billing?

Fortumo is a mobile payments company that enables direct carrier billing with more than 350 mobile operators in 90+ countries. Fortumo's payment products work across a wide range of platforms including desktop devices, smartphones, feature phones, tablets and smart TV-s. These products give consumers a simple, 1-click payment method to charge online purchases to their phone bill. For app stores, digital media companies and game developers, Fortumo provides one integration with 350 mobile operators as well as a single point of contact for settlements, reporting, support and infrastructure upgrades. Founded in 2007, Fortumo has offices in Estonia, San Francisco, Beijing, Delhi, Singapore & Hanoi and is backed by Intel Capital and Greycroft Partners.

https://fortumo.com
https://facebook.com/fortumo
https://twitter.com/fortumo
https://www.linkedin.com/company/fortumo-ltd.