# Direct Debit Duplication, Incident on July 27th, 2020 (GL-IN-776)

StashAway Malaysia Sdn Bhd (201701046385)

**Approval of report**

| Document v1.0 | | | |
|---|---|---|---|
| Author | Nino Ulsamer<br>StashAway Group CTO | Prepared on | 30 July 2020 |
| Reviewed by | Nandini Joshi<br>StashAway Group COO | Reviewed on | 30 July 2020 |
| Reviewed by | Wai Ken Wong<br>StashAway Country Manager Malaysia | Reviewed on | 30 July 2020 |
| Approved by | Steve Kucia<br>Curlec Director | Approved on | 30 July 2020 |
| Approved by | Michele Ferrario<br>StashAway Group CEO | Approved on | 30 July 2020 |

**Version control**

| Version | Date | Reason for change |
|---|---|---|
| v1.0 | 30 July 2020 | Initial version |

**Summary**

On Monday, 27 July, 2020, on behalf of customers who had given the instruction to debit money from their bank accounts, StashAway was supposed to send more than 1,500 direct debit collection requests that were grouped into 7 batches for submission to the third party direct debit provider, Curlec. During the submission of the batches to Curlec, timeouts occurred on Curlec's API that resulted in a retry of the batch submission by StashAway for a total of 26 times for batches 1 and 3-7, and 27 times for batch 2. However, the attempts were in fact all successfully processed by Curlec, resulting in a total of more than 40,000 direct debit collection requests, instead of approximately 1,500, handed over for processing to the banks. Of those, around one quarter were actually processed by the banks and monies received on StashAway's accounts the next day, while the remainder were unsuccessfully processed on the banks' side. Customers who had multiple collection requests scheduled for the day were affected multiple times, respectively. The funds were received on StashAway's account on 28 July (next day, Tuesday) and were immediately refunded back to customers and received by 1,174 customers on the same day by 11pm. Forty-two customers received their money on 29 July, and the last eight customers are due to be refunded by 11pm on July 30.

**Description of events**

Weeks before the incident, on June 1, 2020, StashAway informed the Curlec team of an issue during the direct debit collection process whereby a number of collection requests were not processed correctly after the Curlec system responded with an error message. The issue arose due to the higher-than-normal volume of requests to be processed, as many customers schedule monthly recurring direct debit requests for the first day of the month.

An analysis of Curlec's side revealed that the system was designed to handle a maximum of 99 batches, so when more than 99 batches were submitted, a failure occurred due to a timestamp (that was tracking time only up to the second) as the unique identifier (ID) for the batch within their system. This resulted in assigning the same ID, and so one of the batches would not get processed at all. StashAway would then manually resubmit the batch that was not processed correctly, resulting in manual and error-prone work for StashAway's tech and operations teams.

At the time, StashAway was batching collection requests to be sent to Curlec in batches of 20 requests per batch. These limits had been discussed and agreed with Curlec's tech team during the implementation and testing phase of the system. Because this resulted in a high number of batches to be sent per day, there was a higher and higher chance of the aforementioned Curlec ID conflict to happen as the number of daily collection requests kept growing on StashAway's side.

The Curlec team therefore requested the batch requests be throttled at a rate of 1 request / minute in order to avoid the described issue until they have addressed the existing bug in their system pertaining to the ID conflict.

On StashAway's side, however, it would have been difficult to implement the requested throttling without severely impacting the total time it would take for all collection requests to be processed, potentially affecting the sensitive time until customer monies get invested on StashAway's platform. The Curlec team subsequently shared that collections could be sent in larger batches thus reducing the number of batches to be sent and with it the likelihood of ID conflicts.

The StashAway team asked to confirm the number of collections that could be sent in parallel within a single request, to which the Curlec team replied that the system had been tested to receive up to 5,000 collections per batch without issues, and that another customer was using it with 200 collections per batch. To be conservative, the StashAway team decided to send 250 collections per batch going forward. The system changes were deployed on 20 July at 10:00am and came into action on 21 July.

During the first week of operation, no anomalies were detected and all systems functioned as expected.

However, on 27 July, when attempting to send the daily collection requests, StashAway's systems recorded Curlec server timeouts during the communication with their servers. At that time, though unclear why, Curlec's server CPUs were overloaded which resulted in a slow processing of the requests sent to their servers and, after 3 minutes, a 504 Gateway Timeout error was returned to StashAway. The 504 Gateway Timeout error encountered by StashAway's system triggered a retry logic - the system waits for 120 seconds and then the request is sent again. However, what wasn't communicated was that in the background, the processing continued, and after 3½ minutes the files were ultimately successfully processed on Curlec's end. As Curlec's systems did not deduplicate requests across batches of data these collection requests were processed as additional requests.

On 27 July at 3:36pm StashAway's client service team became aware of an issue where customers were complaining about duplicated direct debit requests being made to their bank account. The tech and operations teams went on a phone call at 3:45pm to start an investigation into the issue and decided to turn off the system that was sending the duplicated requests at 3:52pm. By then, a total of 26 or 27 duplicated batches (depending on the batch) had already been sent over to Curlec's system for processing. StashAway's operations team called Curlec at 4:15pm to understand the root cause of the issue and to try and stop the collection requests from being processed further. The StashAway team subsequently gathered more information and created an incident ticket at 5pm to discuss next steps to take.

The collection requests had already been handed over to the various banks for processing by Curlec, so it was impossible to stop the collection process at that point in time. The team shifted their focus to managing customer complaints and setting up the process for refunding the incorrectly debited monies as soon as possible. At 8:20pm on 27 July an email was sent to all affected customers informing them about the incident and assuring them that their money would be returned to their bank accounts by 11pm on 28 July.

The next morning, on 28 July, the operations team received status updates of the collection requests in two parts: the first part at 9am and the next one at 12pm. The collection requests were filtered into successful and unsuccessful ones, and the successful requests (for which money had already reached StashAway's bank account) were collected into a file and prepared by the operations team for reversal back to the customers. Unsuccessful attempts had failed to debit money from customers' accounts in the first place, and so no action had to be taken. The reversals were sent out at 1pm for the first part and at 3pm for the second part respectively. Amounts of less than RM10k were sent using Interbank GIRO (IBG), scheduled to arrive on customers' accounts by 11pm the same day (on the 28th), while amounts over RM10k were sent using RENTAS for faster processing - these were received within a few hours of sending. The RENTAS payment method is only available for transfer amounts of more than RM10k, so StashAway was unable to

refund smaller amounts in a shorter amount of time.

As of 28 July, 11pm, 1,174 affected customers were reimbursed completely. For 50 customers the initial refund attempt had failed due to errors in the uploaded refund file. This manual error for these 50 clients is also in scope of what StashAway must prevent in the future. Out of those 50 customers, 42 have been refunded by 29 July 11pm. By 30 July, 11pm, all customers are expected to be reimbursed completely.

**Root cause analysis**

After learning about the incident StashAway's tech team immediately began an extensive analysis of the underlying factors that contributed to the occurrence of the events on 27 July. During this process the team worked closely with the direct debit provider, Curlec, to identify issues and work out a joint solution plan.

Contributing factors to the events:

- [Curlec] System overloaded by CPU: The systems were not scaled to manage the expected load in an appropriate manner.
- [Curlec] CPU utilization alerting was configured to trigger at 95% threshold only thus Curlec's team was unaware of the performance issues of their servers.
- [StashAway] Retry logic: StashAway's system attempted to re-submit requests when it was difficult to reason about the status of the previous submission. The system should have stopped and reported an error instead of silently retrying the submission again.
- [Curlec] Lack of deduplication: Even though the collection request includes a unique ID for each collection, Curlec's system did not deduplicate requests that were received from StashAway across batches.
- [StashAway, Curlec & Receiving banks] Lack of rate limiting / suspicious transaction monitoring: No review of unusual number of collection attempts per direct debit mandate in a short timeframe.

**Remediation measures and next steps**

The measures below, on both StashAway and Curlec's sides, will ensure that the submission of duplicate requests will no longer be possible.

- [Curlec] Curlec has increased the CPU capacity of the affected systems for faster processing.
- [Curlec] Curlec has lowered CPU spike protection to start alerting from 95% to 85%.
- [StashAway] StashAway has removed the retry logic that had been present when Gateway Timeout errors are encountered. There are also no retry attempts for any other errors or unclear API responses. Any encountered errors will be logged and alerted to the company's

monitoring systems.

- [StashAway] StashAway has adjusted downwards the number of collection requests to be submitted within one batch from 250 to 150.

- [StashAway] StashAway has implemented a client side deduplication logic whereby before sending any collection requests to Curlec it will pull all transactions of the past 30 days and ensure that none of the collection requests to be submitted have been previously sent to Curlec.

- [Curlec & StashAway] Curlec will temporarily no longer automatically forward uploaded requests to the banks for processing. Instead this step will need to be performed manually, thus introducing human oversight into the collection submission process.

As a further mitigation both for StashAway and other companies using Curlec, StashAway will work with Curlec on the following measures before fully automated operations are resumed:

- [Curlec] Curlec will switch the endpoint that processes collection requests from a synchronous working mode (attempting to process all requests while the HTTP call is active) to an asynchronous working mode (acknowledging receiving of the file as the immediate result of the HTTP call and sending status updates of processing later via a different channel).

- [Curlec] Curlec will implement a deduplication logic based on an additional data field that StashAway will send with each collection request.

In addition to the already implemented oversight and monitoring (shared above), StashAway's engineering team is working on setting up more detailed monitoring dashboards to provide deeper insights into the number of requests processed and errors encountered during processing. These systems will also be configured with automated alerting rules so that respective on-duty operations and tech teams can react immediately when outliers or anomalies are detected. While monitoring had been in place, the respective retry attempts were not captured as they did not result in a failure of the batch process as such.

Until these further measures have been implemented, the automatic forwarding of requests to the banks will be paused as explained above.

**Closing Thoughts**

We do not take lightly what happened this week, and we have set the following immediate priorities for our engineering team:

- **Review alerting for business metrics**
  In order to detect anomalies in a similar way as described for the direct debit collection process, StashAway will review workflows such as deposits, withdrawals, rebalancing, fee charging, and customer onboarding at a granular level. We will establish a set of thresholds to further strengthen the monitoring process and ensure appropriate alerting is in place to notify tech and operational teams of unusual behavior. These thresholds and alerts will proactively mitigate the recurrence of a situation like this happening again.

- **Review of transactional financial service integrations**
  In order to ensure that similar issues such as the one experienced on the direct debit integration side are not going to occur when interfacing with other financial systems such as brokerage or banking systems, StashAway will perform an in-depth review of all of its financial service provider integrations. The integrations will be analyzed for error handling and reporting, retry logics, deduplication logics, monitoring, and alerting. The reviews are scheduled to begin in the week of August 3rd.

We understand that you've entrusted us with your money, and in this case, we did not uphold the very high service and quality standards that we've set for ourselves, and that you have of us. We sincerely apologize for the inconvenience caused towards 1,193 of our customers, and for the concern of those who became aware of the incident. We are doing everything possible to learn from this incident, and are proactively putting in place measures to mitigate the chance of something like this ever happening again.

We set out in 2016 to build a wealth management offering that has security, safety, and risk management at its core. We knew then that wealth management had a long way to go in becoming truly customer-centric, and it was, and still is, our goal to be the most customer-centric wealth manager that you can find. As such, we take our partnerships very seriously, and Curlec's response to this situation is a testament that, in the rare chance that something may go awry, our partners also are jointly committed to serving you.

I hope our response, actions, and transparency with this situation demonstrate our sincere commitment to making sure the money you entrust with us is always safe, and that your experience comes without surprises such as this. We've never taken your trust for granted, and we know we may have a long road ahead to earn back your trust.

In case you have any further questions, please feel free to contact us via email at support@stashaway.my, WhatsApp us at +60 11 1282 9646 or give us a call at +60 3 9212 8536.

Best regards,

Nino Ulsamer
StashAway Co-Founder and Group CTO