

How Swan Bitcoin keeps loss rates down and stays a step ahead of fraud

- ✓ Over 90% reduction in loss rate
- ✓ 80% less time spent on manual review

OVERVIEW

Bitcoin onramp for automatic recurring and instant buys

Swan Bitcoin is a quickly expanding, leading bitcoin savings app that hit the market in March of 2020 in 49 U.S. states. The app started as a gifting service for people to learn more about bitcoin, and has since evolved into an onramp to help consumers understand bitcoin with educational resources, seamlessly set up recurring bitcoin purchases straight from users' bank accounts, help companies purchase bitcoin for corporate treasury, and serve retirement accounts and trusts for long-term savers. Today, Swan is expanding its services to the financial advisor industry as well as employers who are looking to offer a Bitcoin benefit plan to their employees.



Challenge

- Fraudulent orders
- Chargebacks
- Identity reuse and other types of identity fraud



Solution

- Implementing Sift Account Defense
- Leveraging Sift workflows
- Tapping into the network effect of Sift



Results

- Lowered loss rate by 90%
- Reduced manual review time by 80%
- Building new Sift workflows to scale with company growth and fraud patterns



“

What initially drew me to Sift was the number of other partners it integrated with, and the ability to leverage the network effect of Sift across the partner ecosystem. For a startup, leveraging data from others can be a powerful way to enrich your own threat detection data.

Yan Pritzker, Co-Founder & CTO



CHALLENGE

Fraudulent transfers, chargebacks, and identity reuse led to lost revenue

When Swan Bitcoin first launched, the platform experienced an influx of fraudulent transfers, chargebacks, and identity reuse that ultimately led to a significant loss rate. The team identified multiple accounts formed under the same identity, spamming SMS with an influx of phone numbers that made it difficult to keep up with. And although implementing an upfront passwordless login system helped reduce fraud rates, the platform was not entirely free and clear of fraud. Swan recognized they needed a more robust fraud prevention solution to stay a step ahead of the sophisticated tactics they were facing.

But being in the security-conscious Bitcoin space, Swan also wanted to be sensitive to their customers' privacy. Because of these concerns, one-time emails and burner phone numbers are more popular with their users—and likely to be key indicators of fraud in many industries. But for Swan, they could simply be the byproduct of cautious but trusted users looking to protect their identities. This made it especially important for Swan to take into account a larger range of signals, and not apply undue friction to every customer.

After a positive experience utilizing Sift in his previous role at Reverb, Swan's CTO Yan Pritzker decided to implement Sift for Swan Bitcoin. The network effect of Sift was a crucial differentiator, as the large fintech and crypto ecosystem makes it easier to block known malicious entities.

“Sift is instrumental in aggregating data all in one place and making sense of it in a way that's actionable. For a small business, it's really helpful to leverage Sift's signal intelligence and network effect to know if a user is malicious on another site.”



SOLUTION

Implementing Sift Account Defense and optimizing workflows

Within the first couple of months of operation, Swan Bitcoin integrated Sift Account Defense in an effort to get ahead of the fraud they were starting to see across the platform. At first, Swan's fraud team started using score-based workflows and freezing accounts through manual review, gradually introducing limits, and then advancing to workflows to get a deeper understanding of fraud patterns.

Swan utilizes a few key workflows to boost efficiency—one of which is used to trigger manual review when Swan users buy bitcoin for the first time, file a chargeback, or transact in a different country. These higher-risk actions feed into the Sift review queue and the accounts are either limited or terminated, depending on the data compiled in the Sift Console.

To strengthen their efforts, data from multiple fraud prevention vendors, as well as Swan's internal fraud detection metrics, are aggregated into Sift. Swan's fraud agents are able to look at Sift activity logs and correlation data to make the most informed, accurate risk and operations decisions possible. This is especially useful for cases of identity and fingerprint reuse, in which multiple identities are linked to the same device and can be easily shut down altogether. Swan also looks at bank account legitimacy, particularly if the account has an established history of negative behavior. Monitoring and building workflows around ACH reversals have also proved useful for Swan, as some reversal codes are more likely to be fraudulent. are linked to each other, and see user activity including if those users have been flagged in the past under different accounts.

Although the Swan team does its best to accommodate and enable most users, there can be false positives where trusted customers are mistakenly flagged as fraudulent. This is where score thresholds come into play, with scores above a certain threshold being more likely to be fraudulent. Scores in the mid-range are given account limits so they have time to monitor user activity before making a rushed or uninformed decision, reducing the risk of false positives.



RESULTS

Lowered loss rate, reduced manual review time, and boosted efficiency

The aggregation of data in the Sift Console helps empower Swan fraud agents to make accurate and efficient decisions. Swan's fraud reduction efforts have also become more advanced and sophisticated with Sift workflows and automation, making it easier for the platform to prevent fraud. Since implementing Sift, the team reduced the amount of time spent reviewing accounts by 80%, eliminating the need to hire additional agents. And moreover, Sift helped drive Swan's loss rate down by over 90%.

Sift has also helped Swan with an SMS attack in which random accounts, fake emails, and randomly generated domains infiltrated their systems. Swan was able to feed these signals into Sift and automate decisions to shut down the accounts before they could enter the platform and do any more damage.

As Swan continues to grow, Sift has scaled with their needs, ingesting increased data, and improving accuracy. The Swan fraud team continues to iterate and uplevel their Digital Trust & Safety efforts with Sift, building workflows as new fraud patterns emerge to reduce manual review time and keep fraud rates low.

“ Sift is the center of our fraud universe and the lifeblood of our fraud team.

Yan Pritzker, Co-Founder & CTO

ABOUT SIFT

Sift is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of one trillion (1T) events per year, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Poshmark, and Twitter rely on Sift to gain a competitive advantage in their markets.

Visit us at sift.com and follow us on [LinkedIn](#).