SHAPE
Part of F5

CASE STUDY

F5 Helps N.A. Credit Union Improve Its Customer Experience by 99%

At the same time, fraud losses plummeted by 84%

COVID 19 has accelerated the digital shift by at-least two years, with some estimates pointing to as much as a five year acceleration. As credit unions move more of their operations online, they have become an easy target for fraudsters due to a lack of sophisticated fraud controls like those in place at bigger players in the financial services sector. At the same time, not negatively impacting the online customer experience is also an important point for credit unions looking to keep their customer acquisition, engagement and retention metrics in check.

This case study discusses a credit union that saw an astonishing 99.5% reduction in friction around the online customer experience for its members, while preventing 84% of fraud losses using F5's anti-fraud technology.

Credit Unions in the Digital Era

As per BAI*, an independent non- profit organization, "digital banking is moving out of the "early majority" curve and into the "late majority" phase of technology adoption."In their research BAI found that over half of banking customers use digital products more since the pandemic, and that 87% of them are planning to continue this increased usage after the pandemic. This creates an increased digital attack surface for fraud. The pandemic has also resulted in increased efforts to steal customer information via methods like smishing/phishing, social engineering scams, and other methods. Combating this activity requires a holistic fraud solution that simultaneously reduces fraud and improves the online customer experience.

Amidst the digital shift currently underway, credit unions are, unfortunately, perceived by fraudsters to be softer targets than big banks. This is largely because credits unions usually have more limited investments in fraud prevention technologies compared to larger financial institutions.

Pressure to provide the same services as the big banks is pushing credit unions into the uncomfortable position of providing online banking services, but without the requisite cyber security and fraud infrastructure required to adequately protect those online services. In addition, credit unions are also struggling to provide a good online experience to their members across various digital touch-points.

Fortunately, F5 has an affordable, turnkey, easy-to-deploy managed security and fraud solution tailor-made for credit unions.

The Customer: A North American Credit Union

A North American credit union with over $10B in AUM was looking to cut losses incurred due to online money transfer payment fraud that was happening as a result of account takeovers.

THE PROBLEM: INCREASED ACCOUNT TAKEOVERS LEADING TO HIGH MONEY TRANSFER FRAUD

Due to COVID 19, this credit union was seeing heightened digital activity. Like many financial institutions, this credit union's fraud losses were mounting.

Fraudsters took over the customer's account and conducted several fraudulent money transfer transactions via their online digital web and mobile channels. Fraudsters were able to bypass the credit union's existing authentication measures and device identifier solution. The fraudsters then conducted the money transfer fraud and siphoned the funds to mule accounts, leaving the credit union's customer accounts drained of funds.

Below is how Account Takeover and Money Transfer Fraud happen:

Figure 1: Account Takeover and Money Transfer Fraud

In one of its press releases, Juniper research*** talks about a study it did which has found that businesses across various verticals including eCommerce, airline ticketing, money transfer and banking services, will cumulatively lose over $200 billion in the next 5 years. The press release also states, “The research also found that digital money transfer is a growing area for payment fraud, with losses growing by 130% from 2020 to 2024.” Not only was fraud rising rapidly at the credit union, but measures to counter fraud losses were ineffective as well. The credit union was also subjecting its members to unnecessary friction in form of multi-factor authentication (MFA) at login. This resulted in a lot of legitimate customers being subjected to friction during their online experience, while not actually reducing any fraud losses or mitigating any fraud risk.

How F5 Fraud Prevention Solutions Can Help

At this credit union, F5’s anti-bot and anti-fraud technologies helped detect and combat fraud perpetrated due to automated bot attacks as well as fraud performed manually by fraudsters.

When F5’s anti-bot technology was deployed, F5 detected that 40% of the transactions at login were actually the result of malicious automation due to credential stuffing.

Credential stuffing occurs when cybercriminals use stolen user credentials from one application and test those credentials on another application. Attackers use advanced automation tools and bots to target the login function of an application, sometimes executing billions of attacks per day.

Because many users reuse passwords across online services, F5 has discovered that between 0.1%-2% of a stolen credential list will typically be valid on a target site and can lead to account takeover (ATO). And with billions of stolen credentials spilled to and sold on the dark web each year, attackers always have a wealth of credentials to use in ATO attacks.

F5 identified that sophisticated automation attacks resulted in widespread hijacking of accounts for this credit union and was able to detect and block them in real time.

When F5’s anti-fraud technology was deployed, it was able to detect significant fraudulent activity for the credit union. F5 detects online fraud claims using user behavior, environmental, device, and network signals that were seen associated with fraudulent activity. Here is a sample of the anomalies we saw via the hundreds of proprietary signals we collect and analyze, helping us save our customers tens of millions of dollars in fraud losses. The anomalies F5 discovered, based on the telemetry we collected and analyzed, included:

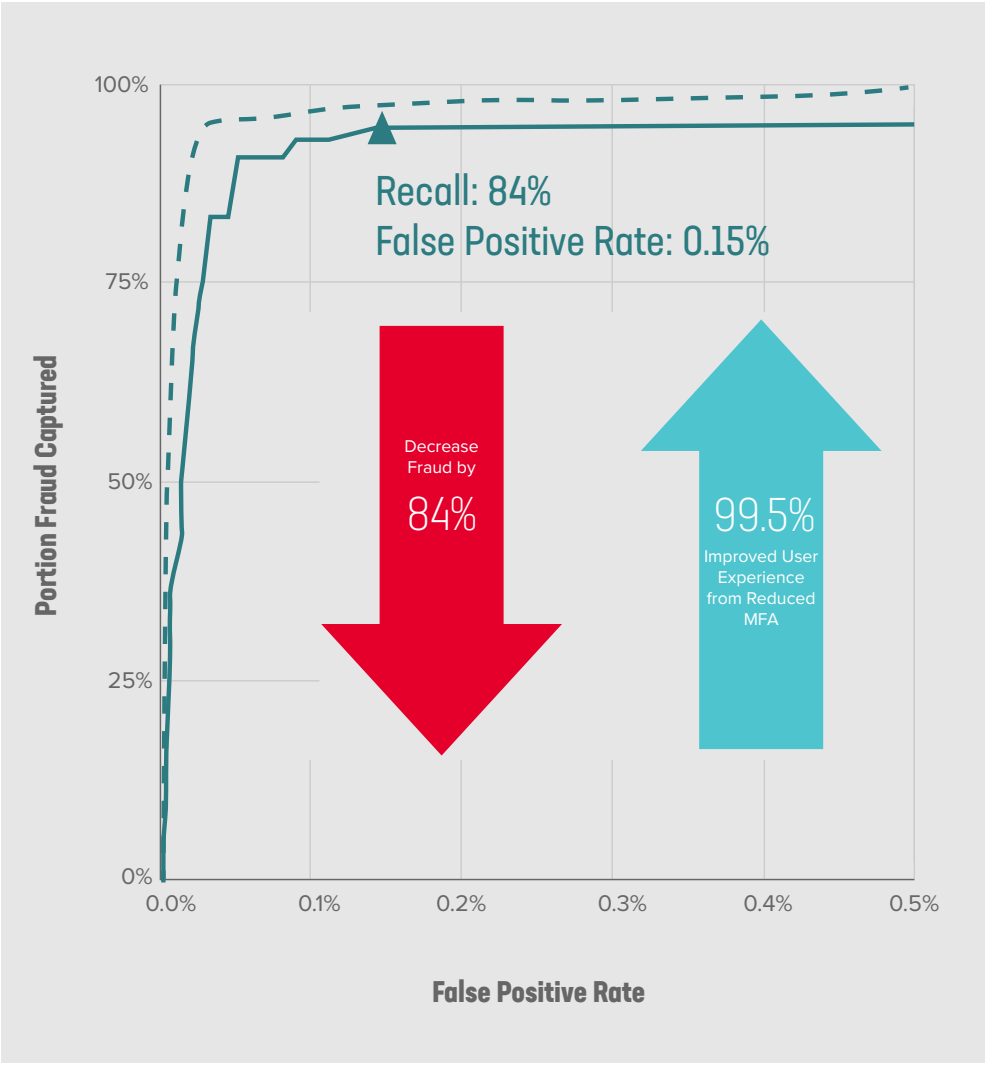
- Copying and pasting activity: Fraudsters were observed routinely copying and pasting data into the login form fields, whereas legitimate users typically do not exhibit this behavior
- Screen toggling: Fraudsters were observed toggling between the browser window and another window, presumably used to cut and paste from a list of stolen credentials.
- Odd screen real estate usage: The fraudster's browser window left quite a bit of screen real estate available, presumably to allow for the list of stolen credentials to appear in a text file beside it.
- Device affinity: On multiple occasions, a large number of member logins were observed coming from the same device.
- Environment spoofing: Fraudsters were observed trying to hide and disguise their respective environments (e.g., browser user agent, OS version, application versions, etc.). As a top contributor to JavaScript , F5's anti-spoofing capability is one of the most mature in the market.
- VPN usage: In many cases, the fraudsters logged in from VPNs, which is yet another method that fraudsters use to hide and disguise themselves.

Results and Return on Investment

The results seen by this credit union were definitive and showed an incredible return on investment (ROI) in the form of significant fraud loss reduction, reduced user friction, and an extremely low rate of false positives for the credit union:

1. Detection and real time blocking of malicious automation (40% of login traffic)
2. Additional annual fraud detection: 84%
3. Reduction in user friction/unnecessary MFA challenges: 99.5%
4. Extremely low false positive rate: 0.015%

Figure 2: Portion of fraud captured and false positive rate



With these results, this credit union quickly realized the value of its investment in F5's technology and is now enjoying the benefits of improved fraud detection and reduced fraud loss with no detrimental impact to business operations, along with a markedly improved online user experience for its members.

To learn more, contact your Shape Security or F5 representative, or visit shapesecurity.com or f5.com.

* https://www.bai.org/banking-strategies/article-detail/covid-19-pushes-digital-banking-adoption-to-the-tipping-point/
** https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion
*** https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion