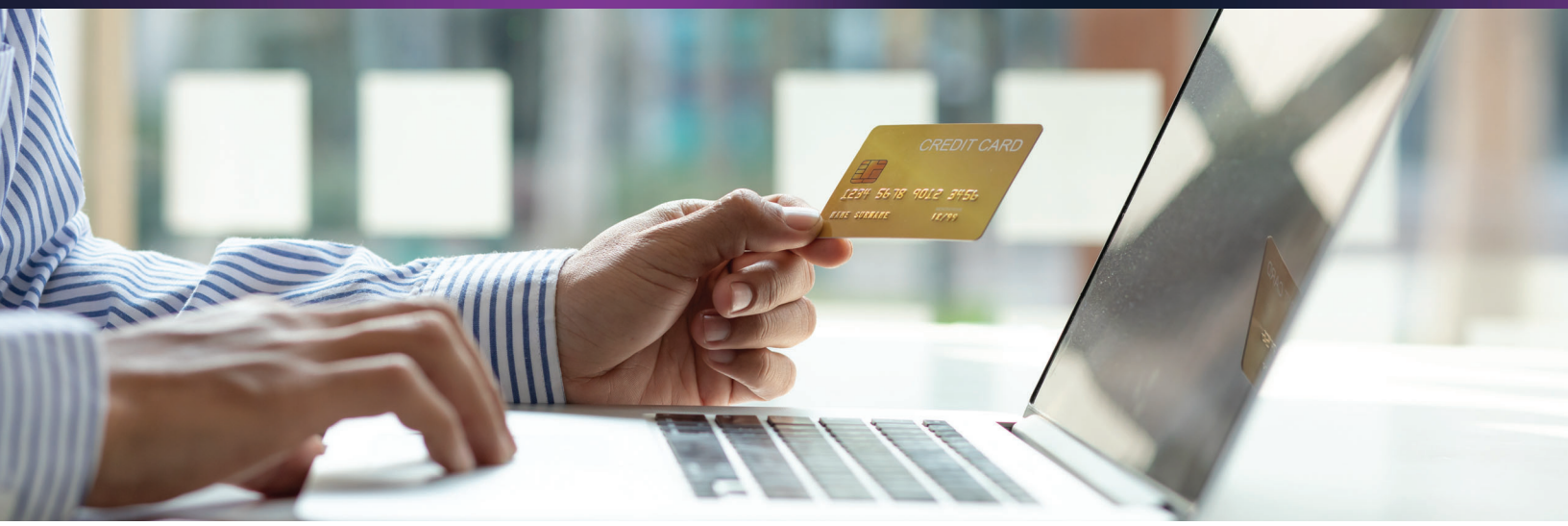
ALLURE SECURITY

HOW A REGIONAL BANK GOT AHEAD OF ONLINE BRAND IMPERSONATIONS TO PROTECT THEIR BRAND & CUSTOMERS



AT A GLANCE

OBJECTIVE

- Proactively detect and remediate online brand impersonations before customers fall victim

CHALLENGE

- Scam websites going unnoticed until months after they'd gone live and victimized customers
- Unhappy customers reporting scams (that traditional domain monitoring alone missed)
- Executives needed assurance the problem was being handled proactively

SOLUTION

- Allure Security's brand protection-as-a service and its mix of AI-powered detection, uniquely effective response capabilities, and web beacons to find and eliminate fake websites

RESULTS

- Detection and eradication of brand impersonation attacks before customers fell victim gaining a "proactive edge on the bad guys"
- Improved takedown efficiency – reduced from months to hours
- Estimated detection & disruption of 3 malicious websites a month with an average takedown time of less than a day

CHALLENGE

ELIMINATING THE PRECURSOR TO PHISHING AND FRAUD

A regional bank managing $30 billion in assets and serving the New York metropolitan area had experienced an increase in scams targeting its millions of customers. Fraudsters impersonated the bank's brand online by cloning its websites, sent phishing e-mails directing the bank's customers to the malicious sites, and tricked victims into entering their credentials. With these stolen credentials the fraudsters then took over customer accounts and stole their money.

The bank had implemented a domain monitoring system, however, customers still called into the bank complaining of scams the system missed. The bank's cybersecurity and threat management team demanded a better way. The team wanted increased visibility into online threats impersonating their brand and targeting their customers. Second, they wanted to identify these scam websites closer to their original creation to head-off phishing and related fraud before it occurred.

CONTACT US FOR A FREE TRIAL
info@alluresecurity.com

alluresecurity.com
877-669-8883

SOLUTION

SPOTTING AND ADDRESSING FAKE SITES IN HOURS VS. MONTHS

The bank chose Allure Security's AI-powered online brand impersonation detection engine, its unique anti-cloning web beacons, and its unparalleled threat research and response team to identify and address fake websites more quickly than they could previously. The bank's domain monitoring solution would identify some problematic websites months after they went live, which the director of cybersecurity described as "...useless to us."

The early stages of a phishing campaign consist of the scammer registering a domain, copying the bank's website content to it, and then publishing the page. The bank's Director of Cybersecurity & Threat Management appreciated Allure Security's ability to detect the scam website during these early phases, prior to the launch of the phishing campaign and before any customers fell victim.

He described the thought process of a fraudster they were now able to spot more quickly as follows, "Wow, I didn't expect that to happen. They cut my operation off at the knees."

Allure Security delivers brand protection as a service and its web beacons take mere minutes to implement. As a result, the bank had immediate insight into the origins of brand impersonation attacks against their bank and users accessing their web content – whether authorized or unauthorized.

> *"If there are fake sites out there, that's a direct reputational issue for us because somebody's using our brand to do something fraudulent. We take customer safety and security online very seriously…The product has been tremendously useful."*
>
> *— Director of Cybersecurity & Threat Management, $30B Regional Bank*

RESULTS

With the new technology and approach in place, the cybersecurity and threat management team felt confident they now had an edge on scammers targeting their customers and were no longer flying blind. As the director of cyber security put it, "[Now] leadership has a good level of understanding of the problem. They know this is something that we have eyes on. They know we have the capabilities to detect it."

Overall, the team significantly reduced mean-time-to-detection of brand impersonation attacks (i.e., how long an impersonation is accessible before it's discovered). This improved detection combined with transferring mitigation responsibilities to Allure Security's expert Threat Research & Response team also significantly reduced mean-time-to-response (i.e., the time it takes to eliminate a threat once it's discovered) – in some cases reducing it from months to hours.

The new technology also enabled the team to identify and extinguish a network of fake websites used to execute a loan application scam that stole victims' banking credentials and money. The team also found a scam website in an unexpected place, buried deep within a Vietnam coffee shop's compromised website. Fortunately, the bank caught the fake website as the scammer, based in Nigeria, provisioned it and before any customers were directed to it. Without Allure Security's detection and response capabilities, both of these scams would have gone unnoticed and unmitigated.