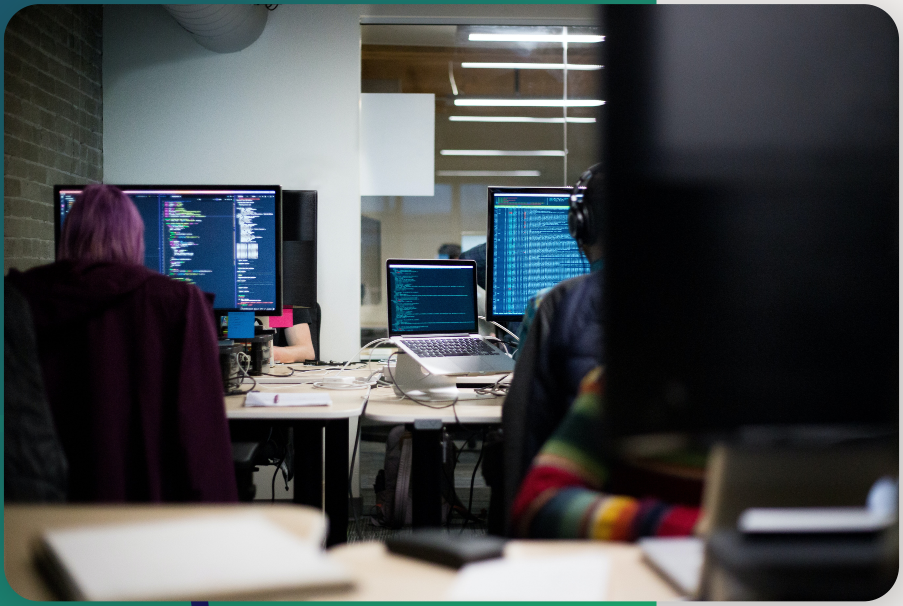
DATA SHEET

Outseer FraudAction™

Protect your customers and business
from external fraud threats



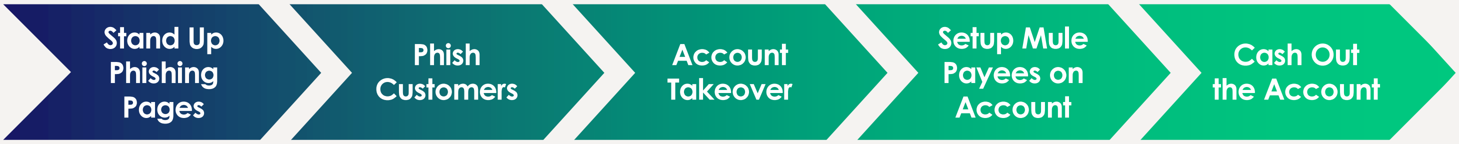
OUTSEER

READ ON

Outseer FraudAction™

Outseer FraudAction protects your customers beyond your firewall by combining cybercrime focused cyberintelligence and industry-leading takedown services to find and neutralize phishing, malware, and brand abuse. FraudAction stops attacks on your customers before their credentials are phished, and long before attackers take over accounts and your business books losses. When combined with the full suite of Outseer solutions, like Fraud Manager to protect authentication, and 3DS to protect card-not-present online transactions, you can intercept fraud at many points along the attack chain, reducing losses and protecting customers.

Account Takeover: Anatomy of a Phishing Scam


Stand Up Phishing Pages

Phish Customers

Account Takeover

Setup Mule Payees on Account

Cash Out the Account

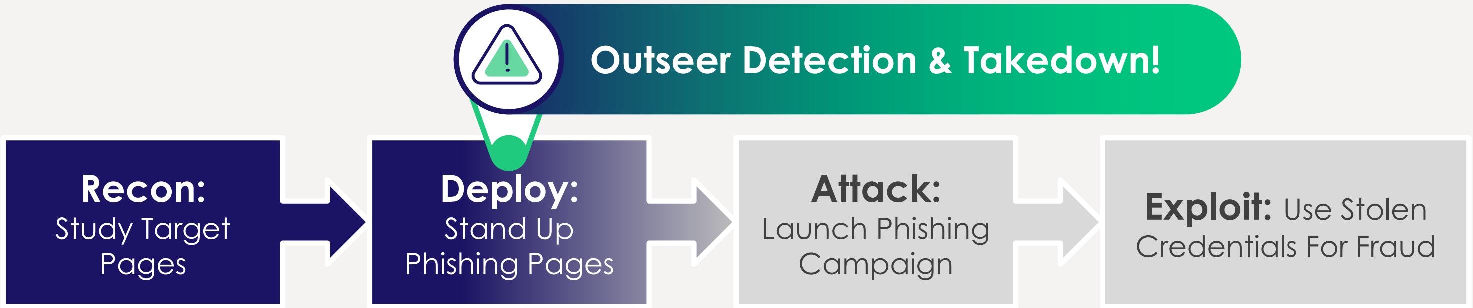
Attack the Attack Chain

Fraud depends on a series of linked steps. To cash out an account, you need control over the account. To gain control over an account, you need customer login credentials. To get customer login credentials, you need to trick the customer into sharing their credentials. Each step depends on everything “going right“ for the fraudster. If any "link“ in the chain of events is broken, the entire chain fails and the attack fizzles. If we make efforts to disrupt every link in the chain, the odds of successful fraud drop precipitously.

In the case of an account takeover (ATO), the earliest point in the chain for us to target is the phishing campaigns targeting customers. That is exactly what FraudAction is built to do. By tracking domain registrations and ownership changes, we can predict which pages will be used for phishing. We monitor those pages carefully – when the domain is inevitably used for phishing, FraudAction is already prepared to start the takedown. Phishing attacks can be disrupted before more customer credentials are breached – and in some cases, disrupted before the phishing campaign is even launched. FraudAction gives you the initiative, forcing fraudsters to react to you.

By taking every opportunity to disrupt fraud, and by focusing on stopping as much fraud as possible as early in the attack as possible, FraudAction can lower the cost of responding to fraud. Disrupting phishing before customers get phished means fewer customers lose credentials. That translates to less operational expenses spent reaching out to breached customers who need to reset passwords, lower ATO losses, and a better overall customer experience.

Attack the Attack Chain with Outseer FraudAction™


Outseer Detection & Takedown!

Recon: Study Target Pages

Deploy: Stand Up Phishing Pages

Attack: Launch Phishing Campaign

Exploit: Use Stolen Credentials For Fraud

Brand Protection and Scam Disruption

Phishing login credentials is just one avenue to victimize your customers. Many fraudsters leverage the trust that customers place in your brand to solicit a customer's personal information or promote scams. Brand abuse frequently spreads on social media, claiming to offer rewards like gift cards in exchange for providing information. Pilfered information can be sold to spammers or used to support fraud schemes that specialize in victimizing your customers. Scams directly steal from your customers, leaving them confused – and angry at your firm.

According to research by FINRA and the BBB, 90% of consumers that report brand abuse on social media engaged with brand abusing content[1]. Customers are not always aware of the difference between authorized branded content and brand abusing content, and they may publicly blame the company for allowing brand abuse on social media. Scams and targeted fraud enabled by brand abuse is very costly when it targets your business. Typical schemes are credit fraud schemes and call center account takeover fraud. Fraud targeting your customers directly can impact your bottom line by proxy. If customers lose money to scams, they have less capacity to do business with your company.

The FraudAction Detection network is vigilant to brand abuse, rogue apps, and scams targeting your customers with your brand. With twenty years of experience, and by leveraging over 10,000 relationships with social media firms, ISPs, and registrars, we can assist in takedown for these pernicious threats to your customers.

"90% of consumers that report brand abuse on social media engaged with brand abusing content"

Intelligence-Led

FraudAction Cyberintelligence (FACI) complements our takedown services and other Outseer products by maintaining a presence on cybercrime forums and by engaging with criminal actors to track new and emerging threats to your brand and customers. We collect breached credentials and breached information. We hunt for stolen credit card numbers and schemes to harm your customers. You may not be aware of data breaches and stolen data until you see headlines in the news – but FACI aims to give you advanced warning. With more and more firms relying on trusted third-parties to support their businesses, and with supply chain attacks on the rise, being alert to breached data is more important than ever in the fight against fraud.

No-Code Implementation

Once you engage FraudAction, we enroll your brands into our Detection Network within days. FraudAction can autonomously identify threats to your customers and brand, and initiate takedown of malicious phishing sites and malware distributing sites. There is no code to change to initiate protection. FraudAction does offer more advanced services like abuse mailboxes, referral-tracking pixels, and API data feeds that can offer more integrated solutions to protect your customers.

Sources:

1. Reported Brand Abuse | **Finra**

About Outseer

Outseer is on a mission to liberate the world from transactional fraud. Our market-leading payment and account monitoring solutions protect over $200 billion in annual payments while increasing revenue and reducing customer friction for card issuing banks, payment processors, and merchants worldwide. Leveraging billions of annual transactions from more than 6,000 institutions across the globe, our identity-based science delivers the highest fraud detection rates and lowest customer intervention in the industry. See what others can't at outseer.com.

OUTSEER