# HOW A GLOBAL FINANCIAL SERVICES COMPANY STOPPED BRAND IMPERSONATION ATTACKS ON SOCIAL MEDIA

## AT A GLANCE

### OBJECTIVE

- Remove social media profiles impersonating the brand and executives

### CHALLENGE

- Limited visibility into impersonation attacks targeting their brand and customers across the web and social media
- Lack of proven method for removing deceptive social media profiles

### SOLUTION

- Allure Security brand protection-as-a-service detected and mitigated more brand impersonations on social media more quickly before customers fell victim

### RESULTS

- Dozens of malicious social media profiles identified within one hour
- Hundreds of deceptive profiles identified and removed before customers fell victim
- Reduction in fraudulent transactions and customer complaints

## CHALLENGE

### BRAND & STAFF IMPERSONATIONS ON SOCIAL MEDIA

A renowned international financial services organization became aware of fraudsters impersonating their brand and employees on social media platforms around the world. The scammers fooled a number of the organization's customers into believing these social media profiles were legitimate and ended up stealing personally identifiable information and money from the victims.

At the outset, the organization lacked visibility into the extent of the problem. They didn't know how to find these brand impersonations across the entire internet. Even if they could find the scams, they didn't know how to efficiently and effectively stop them. Each minute that passed further damaged their brand and credibility and led to more customers falling victim. For help addressing the problem and its magnitude, the financial services organization approached Allure Security.

# SOLUTION

### AI-POWERED ONLINE BRAND IMPERSONATION DETECTION

The Allure Security team sprang into action immediately, training its AI-based detection engine to recognize legitimate and illegitimate uses of the brand name, brand imagery, brand messaging, executives' names and photos, and more. Within an hour, the engine had identified more than three dozen deceptive social media profiles impersonating the brand and its executives' likenesses on Facebook, Twitter, and Instagram.

Because Allure Security delivers brand protection as a managed service, the financial services organization immediately increased their visibility into brand impersonation attacks with little-to-no effort on their part.

### PREEMPTING FRAUD WITH PROACTIVE DETECTION

In addition to the three dozen malicious profiles originally discovered, Allure Security's detection engine found more than 200 additional Twitter and Facebook profiles using variations of the company's logo, taglines, and other branding. Scammers had created these deceptive accounts, but not yet made use of a majority of them. Allure Security identified these scams before they lured a single victim – saving untold amounts of time, effort, and customer goodwill.

### DILIGENT RESPONSE, FOLLOW-UP & TAKEDOWN

As the Allure Security detection engine scoured the internet and social media platforms for more impersonations, our security operations team began its work to remove the deceptive profiles from the platforms. With a history of successful removals of fraudulent social media profiles, the team followed its proven social media profile removal methodology:

- Packaging up evidence to substantiate the claim that the impersonators were violating the relevant social media platforms' terms of service
- Properly documenting Allure Security's role as an authorized representative of the financial services organization and our authority to request removals on behalf of the company
- Submitting deceptive profiles and following-up digitally with the social media platforms to ensure the content was taken down and remains inaccessible

# RESULTS

In the end, the financial services organization offloaded brand protection efforts to Allure Security resulting in the detection and disruption of more online brand impersonations more quickly. The company no longer had to rely on customers to report online brand impersonations once the fraud had already occurred. Proactive detection, a proven removal process, and diligent follow-up from Allure Security significantly reduced the time it took to detect and address brand impersonation attacks. This correlated directly to a reduction in fraudulent transactions and customer complaints about online scams related to the brand.

The financial services company continues to protect its brand across digital channels – including the web, social media, and mobile apps – with Allure Security able to find and eliminate online scams as they arise. This proactive approach reduces online fraud and digital risk and prevents expensive incident response procedures, lost sales, customer dissatisfaction and churn, and damage to a company's brand and reputation.