proofpoint.

PROMINENT MULTINATIONAL BANK PROTECTS BRAND AND CUSTOMERS FROM SOCIAL MEDIA FRAUDSTERS

CHALLENGES

- Identify all accounts linked to the brand on social—both legitimate and malicious

- Manage a high volume of messages to review for harmful content across its corporate social media accounts

- Protect customers from angler phishing attacks

SOLUTION

- Proofpoint Social Patrol

- Proofpoint Social Discover

- Proofpoint Angler Phish Protection

RESULTS

- Identified over 725 accounts linked to the brand, including over 80 fraudulent, protest, and unauthorized accounts

- Automatically moderated 286,000 posts for harmful content and compliance violations

- Generated real-time risk alerts for 6,014 acceptable use, 1,165 security, and 304 compliance incidents

- Stopped angler phishing attacks that could have resulted in customer account compromise

- Protected corporate brand reputation and sensitive customer account data

OVERVIEW

Not many banks can say they tamed the American frontier, survived the Great Depression, and led the industry into the Internet Age. So when a financial services company—now one of the largest in the world—looked to branch out into social media, it was shouldering the weight of a 160-year history.

Throughout this storied past, the bank has maintained two core values: reliability and trust. Protecting customers and their assets is critical—not just in the physical world but online and in social media.

Today, the company operates across more than 30 countries and has 70 million customers globally. It provides a full range of services for consumers, businesses, and government entities. It has quickly grown its presence across leading social media platforms to acquire, engage, and support customers. The goal: market services, promote community outreach, and provide a new customer-service touchpoint.

THE CHALLENGE

As the corporate marketing team looked to manage the bank's social media activity, it faced three big challenges.

The first was account sprawl. As a regulated entity, the bank must supervise account content for compliance risks. Accounts had been created for various business units, services, and branches. Finding them all—let alone watching for and resolving compliance issues—required manual searches. The job grew exponentially harder with each new account.

The second challenge was providing a good customer experience. The bank's large social media audience is a big draw for bad actors. The explosion of spam, political posts, and other unwanted content quickly outpaced the bank's ability to remove it.

Customer safety was the third and most acute challenge. The bank had discovered angler phishing attacks against customers. This type of attack is named after the anglerfish, which uses a glowing lure to bait and attack its prey. In the same way, angler phishing attacks use fraudulent customer support accounts to steal customer information.

During business hours, the bank's customer care account on Twitter provides live responses to customer queries. Once the bank's service account closed for the day, attackers with legitimate-looking impostor accounts watched for after-hours service requests. The attackers hijacked those requests, responding directly with bogus support links. The links directed customers to phishing sites, which stole login credentials and personal, financial, and security information.

THE SOLUTION

All three of the bank's social media challenges—poor visibility into its social footprint, a high volume of posts to manage, and angler phishing attacks—were too much for any team to solve manually. It needed an automated approach to keep customers safe.

The bank now relies on Proofpoint's Social Discover, Social Patrol, and Angler Phish Protection products. Social Discover automatically finds

> **"It's important that we proactively identify social media fraudsters to mitigate any issues where customers could have their bank account compromised. Proofpoint gives us that protection"**
>
> AVP of Social Care Service

Automatically moderated 286,000 posts

for harmful content and compliance violations

all social media accounts associated with the brand. Social Patrol automates the process of removing content for security and compliance risks. And Angler Phish Protection detects angler phishing attacks in real time to safeguard social media support requests.

THE RESULTS

The team now has the visibility it needs. Social Discover found more than 725 accounts associated with the bank's brand. The solution scans networks daily to identify any new accounts using the brand—both sanctioned and malicious. Using insights from Social Discover, the bank has reported and taken down more than 80 malicious accounts.

At the same time, Social Patrol's automated content removal keeps the bank's accounts free of offensive language, malware threats, and compliance breaches. The bank has removed more than 286,000 unwanted and malicious messages since adopting Social Patrol. It has also received real-time alerts for 6,014 acceptable-use violations, 1,165 security threats, and 304 compliance issues. Real-time automated content analysis has relieved the team from burdensome, manual reviews of every post.

Angler Phish Protection stops angler phishing in its tracks. Now when people engage with the bank's customer-care team on Twitter, they are kept safe. Proofpoint alerts the bank's Social Care Servicing Team immediately when a fraudulent account tries to contact a customer. The team follows up with its swift incident response process. It alerts the customer and works with Twitter to take down the fraudulent account. With Proofpoint, the bank can support customers securely on social media.

"It's important that we proactively identify social media fraudsters to mitigate any issues where customers could have their bank account compromised," said the bank's AVP of Social Care Service. "Proofpoint gives us that protection."

proofpoint. ™   proofpoint.com