360 fraud protection
by AppGate

360 BRAND GUARDIAN USE CASES

DETECT, DISRUPT, AND DEACTIVATE EXTERNAL THREATS BEFORE THEY DAMAGE CUSTOMER TRUST

A Practical Guide for Financial Institutions

DETECT, DISRUPT, AND DEACTIVATE
EXTERNAL THREATS
BEFORE THEY DAMAGE CUSTOMER TRUST

ABSTRACT

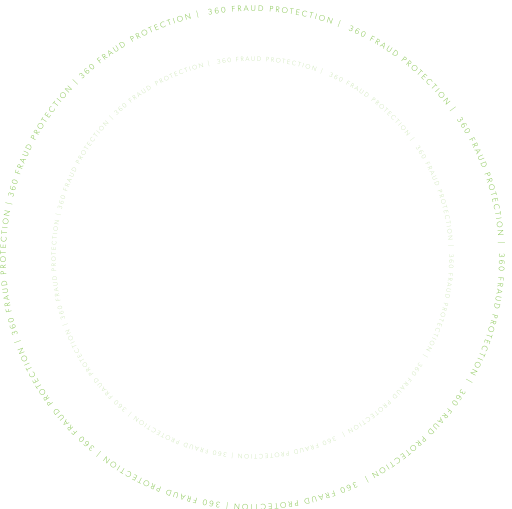
Fraud does not always begin inside a financial institution's digital banking environment. Increasingly, it starts outside the institution's owned channels, across phishing sites, smishing campaigns, fake mobile apps, malicious ads, spoofed domains, social media impersonation, and exposed data circulating across the deep and dark web.

These external threats are not only brand protection issues. They are often the first stage of the fraud chain. A fake login page can lead to credential theft. A fraudulent social profile can mislead customers into a scam. A rogue mobile app can capture sensitive information. Exposed credentials or card data can become the foundation for account takeover, card fraud, or social engineering.

360 Brand Guardian by AppGate helps financial institutions detect, monitor, and deactivate external threats before they scale into customer harm, fraud losses, reputational damage, or operational disruption. Powered by continuous monitoring, AI-driven intelligence, and the 24/7 Guardian Fusion Center, 360 Brand Guardian helps institutions move from reactive takedown to proactive threat disruption.

TABLE OF CONTENTS

1. **Introduction:** External Threats Are the First Stage of Fraud
2. The Brand Guardian Value Story
3. The External Fraud Chain
4. **Use Case 1:** Phishing, Smishing, and Fake Website Takedown
5. **Use Case 2:** Brand Abuse Protection
6. **Use Case 3**: VIP and Social Media Impersonation Protection
7. **Use Case 4:** Deep and Dark Web Monitoring
8. **Use Case 5**: Mobile Threat Protection
9. **Use Case 6**: AI-Generated Scam Disruption
10. The Guardian Fusion Center
11. Customer Proof Points
12. Conclusion
13. About AppGate



01.

INTRODUCTION: EXTERNAL THREATS ARE THE FIRST STAGE OF FRAUD

Financial institutions are facing a new reality: fraud often begins before a customer logs in, before a transaction is initiated, and before internal systems see suspicious behavior. Attackers increasingly exploit the institution's brand, employees, digital presence, mobile channels, and customer trust to start the fraud chain earlier.

A customer may receive a phishing email, a smishing message, or a malicious ad that appears legitimate. They may land on a fake banking website, interact with a fraudulent customer support account, download a rogue mobile app, or see an executive impersonated on social media. These attacks are designed to create trust before they create loss.

Traditional fraud controls are often activated too late in the process. By the time suspicious account activity or payment behavior appears, credentials may already be compromised, customers may already be manipulated, and funds may already be at risk.

360 Brand Guardian helps institutions move earlier in the fraud chain. It continuously monitors external digital channels, detects threats targeting the institution's brand and customers, and supports coordinated takedown and deactivation workflows. The goal is not simply to generate alerts. The goal is to disrupt external threats before they reach customers or escalate into fraud.

02.

THE BRAND GUARDIAN VALUE STORY

360 Brand Guardian helps financial institutions protect the digital trust surface: the brand, the customer, the channel, and the interaction.

1 | PHISHING, SMISHING & FAKE WEBSITE TAKEDOWN

Proactively detect and remove phishing pages, smishing links, and fake websites designed to steal customer credentials.

Continuous Monitoring
Scan web, SMS, and messaging channels 24/7 to detect threats in real time.

Automated Takedown
Trigger automated workflows to remove malicious sites and links quickly.

Protect Customers
Stop credential theft and reduce fraud before users are impacted.

2 | BRAND ABUSE & IMPERSONATION MONITORING

Identify and take action against unauthorized use of your brand, logos, domains, and contentacross digital channels.

Detect & Monitor
Find unauthorized brand use across websites, social media, ads, and marketplaces.

Enforce & Take Down
Enforce policies and remove infringing or impersonating assets.

Protect Your Reputation
Safeguard brand trust and prevent customer confusion and abuse.

3 | DEEP & DARK WEB MONITORING

Gain early visibility into underground activity, stolen data, and threats targeting your brand and customers.

Underground Visibility
Monitor forums, marketplaces, and leaks across deep and dark web sources.

Threat Intelligence
Identify exposed data and emerging threats before monetization.

Proactive Protection
Take action early to reduce risk and protect your customers and brand.

From Fragmented Threat Management

Many institutions rely on disconnected processes to manage phishing, brand abuse, impersonation, mobile threats, and exposed data. Internal teams may depend on customer reports, manual searches, ad hoc escalation, and platform-by-platform takedown requests. This creates several challenges:

- Blind spots across social, web, mobile, advertising, and underground channels
- Delayed response to fast-moving phishing and impersonation campaigns
- High operational burden for fraud, security, marketing, and support teams
- Increased risk of customer exposure before action is taken
- Difficulty proving proactive fraud risk mitigation to executives and regulators

To Unified External Threat Defense

360 Brand Guardian consolidates external threat monitoring and response into a coordinated defense model. It helps institutions detect phishing, smishing, brand abuse, social media impersonation, rogue mobile apps, malvertising, spoofing, malware, and exposed data before those threats create downstream fraud. This approach supports three core business outcomes:

- Prevent fraud losses and reduce operational costs by disrupting scams before they reach customers
- Safeguard brand and maintain customer trust by deactivating external threats faster
- Support secure digital growth by protecting customer interactions across public digital channels

03.

THE EXTERNAL FRAUD CHAIN

External threats can become the starting point for broader fraud operations. 360 Brand Guardian helps institutions detect and disrupt these threats at the earliest stage.

THE EXTERNAL THREAT LIFECYCLE

1 BRAND EXPOSURE

Phishing, smishing, spoofed domains, fake ads, rogue apps.

2 CUSTOMER DECEPTION

Impersonation pages, fake support, social scams, malicious landing pages.

3 CREDENTIAL & DATA CAPTURE

Fake logins, stolen credentials, card data theft, malware delivery.

4 FRAUD ENABLEMENT

ATO, payment fraud, identity misuse, scam monetization.

5 DETECTION & DISRUPTION

Monitoring, takedown, investigation, reporting, risk reduction.

Stage 1: External Exposure

Attackers create or distribute malicious assets outside the institution's owned environment. Examples include phishing sites, smishing links, fake apps, spoofed domains, malicious ads, social impersonation, and leaked data.

Stage 2: Customer Deception

Customers are tricked into trusting the asset because it appears to be connected to the financial institution. Examples include fake login pages, fraudulent support profiles, executive impersonation, fake security alerts, and urgent account verification messages.

Stage 3: Credential or Data Capture

Attackers collect usernames, passwords, OTPs, personal data, card information, or device-level signals.Examples include credential harvesting, malware, fake forms, malicious apps, and social engineering.

Stage 4: Fraud Enablement

Captured data is used to support account takeover, card fraud, payment fraud, identity theft, or mule activity.Examples include credential stuffing, unauthorized account access, card-not-present fraud, payment manipulation, and targeted scams.

Stage 5: Threat Disruption

360 Brand Guardian detects, investigates, prioritizes, and supports takedown or deactivation of malicious assets before they continue to spread. Examples include phishing takedown, social profile removal, rogue app detection, brand abuse enforcement, and deep/dark web intelligence.

04.

USE CASE 1: PHISHING, SMISHING, AND FAKE WEB-SITE TAKEDOWN

Disrupting Credential Theft Before It Becomes Account Takeover

Phishing and smishing remain among the most common ways attackers exploit customer trust. A message that appears to come from the institution can direct customers to a fake login page, capture credentials, and create the conditions for account takeover or payment fraud.

These attacks often happen outside business hours, over weekends, or through infrastructure that changes quickly. Manual reporting alone is not enough. Institutions need continuous monitoring and a response process that can move faster than the scam.

How 360 Brand Guardian Helps

360 Brand Guardian helps institutions detect, validate, and deactivate phishing and smishing infrastructure before exposure grows.

Business Value

Phishing and smishing protection helps reduce credential theft, account takeover risk, customer data exposure, reputational damage, and the operational burden of manually chasing fake websites.

Customer Proof Point: Trax Credit Union

Trax Credit Union needed a hands-off way to proactively monitor phishing emails directing members to fake websites. With 360 Brand Guardian, Trax implemented proactive monitoring and takedown of fake and phishing websites. The solution helped reduce internal time spent chasing threats while providing proactive reporting and 24x7x365 support.

trax CREDIT UNION

COMMON THREAT SCENARIOS

- Fake online banking login pages
- SMS phishing messages with urgent account warnings
- Phishing emails that redirect customers to counterfeit sites
- Malicious URLs distributed through social media, email, SMS, ads, or messaging apps
- Reappearing phishing infrastructure after takedown

THE SOLUTION HELPS INSTITUTIONS:

- Detect phishing attacks using multiple intelligence sources
- Continuously monitor new domain registrations
- Identify malicious URLs and fake login pages
- Support takedown workflows with hosting providers and relevant platforms
- Track progress until the threat is resolved
- Provide reporting for fraud, security, and executive stakeholders

05.

USE CASE 2: BRAND ABUSE PROTECTION

Protecting Brand Trust Across Digital Channels

Brand abuse occurs when attackers misuse an institution's name, logo, trademarks, domain patterns, or visual identity to create credibility for scams. This can happen across websites, social media, app stores, advertising platforms, search results, and other public-facing digital environments.

For financial institutions, brand abuse creates more than reputational exposure. It can become the first step in credential theft, fake support scams, fraudulent promotions, rogue app distribution, or customer deception.

How 360 Brand Guardian Helps

360 Brand Guardian helps institutions monitor for brand misuse and initiate enforcement actions before malicious assets spread.

Business Value

Brand Abuse Protection helps reduce customer exposure, protect digital campaigns and product launches, strengthen brand confidence, and lower the cost of reacting to scams after they spread.

Customer Proof Point: Progressive Bank

Progressive Bank faced counterfeit websites and phishing attempts targeting its customers. The bank needed a lightweight solution that could proactively monitor sophisticated attacks and remove counterfeit websites with minimal ongoing maintenance. With 360 Brand Guardian, Progressive Bank identified unauthorized mobile applications and removed fraudulent activity without involvement from the bank's internal team.

COMMON THREAT SCENARIOS

- Fraudulent ads using brand keywords or trademarks
- Rogue mobile apps misusing the institution's identity
- Websites using brand terms, logos, or visual patterns to mislead customers
- Social media pages impersonating the institution
- Malicious SEO tactics that redirect users to scam infrastructure

THE SOLUTION HELPS INSTITUTIONS:

- Monitor web, domains, app stores, advertising ecosystems, and social platforms
- Identify fraudulent creatives, pages, apps, domains, and impersonating assets
- Prioritize brand abuse threats based on customer impact and risk
- Support takedown and enforcement workflows
- Provide evidence for fraud, security, marketing, legal, and compliance teams

06.

USE CASE 3: VIP AND SOCIAL MEDIA IMPERSONATION PROTECTION

Protecting the People Customers Trust

Fraudsters do not only impersonate financial institutions. They also impersonate executives, board members, customer support teams, relationship managers, and other public-facing individuals associated with the brand.

These attacks are effective because they use authority, familiarity, and urgency to make scams more credible. A fake executive profile or fraudulent support account can direct customers toward phishing sites, fake investment opportunities, fraudulent forms, or malicious conversations.

How 360 Brand Guardian Helps

360 Brand Guardian helps institutions detect and disrupt social media and VIP impersonation threats before they escalate.

Business Value

VIP and social media impersonation protection helps preserve customer trust, protect executives and public-facing employees, reduce reputational risk, and prevent impersonation from becoming a launchpad for phishing or broader fraud campaigns.

Customer Proof Point: FNB Hutchinson

FNB Hutchinson's Marketing team was alerted by a customer who identified a fraudulent Facebook profile impersonating the bank's CEO. The profile was confirmed to be an imposter. The bank opened a case with the 360 Fraud Protection team, and the fraudulent profile was removed within approximately one hour of escalation.

FIRST NATIONAL BANK

COMMON THREAT SCENARIOS

- Fake CEO or executive profiles
- Fake customer support accounts
- Company impersonation pages
- Impersonated relationship managers or public-facing employees
- Social media scams promoting fake offers or fraudulent assistance

THE SOLUTION HELPS INSTITUTIONS:

- Detect fake profiles, pages, and accounts impersonating brands or designated individuals
- Monitor public digital channels for impersonation activity
- Analyze context, behavior, and engagement signals to prioritize response
- Support coordinated takedown actions
- Reduce exposure to trust-based social engineering

07.

USE CASE 4: DEEP AND DARK WEB MONITORING

Detecting Exposed Data Before It Fuels Fraud

Fraud often starts before a phishing message is sent or a fake site is reported. Credentials, card data, customer information, corporate data, and fraud-enabling tools may already be circulating in underground sources.

Deep and dark web intelligence helps institutions identify exposure earlier and understand how stolen information may be used in account takeover, card fraud, credential stuffing, social engineering, or targeted scams.

How 360 Brand Guardian Helps

360 Brand Guardian helps institutions monitor underground sources for compromised data and emerging fraud indicators.

Business Value

Deep and Dark Web Monitoring helps institutions reduce risk from exposed credentials and card data, support proactive investigation, protect customers earlier, and connect underground intelligence to real-world fraud prevention actions.

Customer Proof Point: FNB Hutchinson

FNB Hutchinson uses BIN monitoring through 360 Fraud Protection to identify potential exposure of its card portfolio on dark web marketplaces. When specific customer accounts could be identified, the bank proactively mitigated risk by closing affected debit cards and issuing replacements.

FIRST NATIONAL BANK

COMMON THREAT SCENARIOS

- Leaked usernames and passwords
- Compromised customer information
- Exposed corporate data
- Compromised payment card data
- BIN exposure across dark web marketplaces
- Fraud kits, tools, and indicators linked to active campaigns

THE SOLUTION HELPS INSTITUTIONS:

- Monitor deep and dark web forums, marketplaces, and channels
- Detect leaked credentials, compromised card data, and exposed information
- Identify domain-related threats and fraud indicators
- Correlate underground intelligence with phishing, brand abuse, and impersonation campaigns
- Support early intervention before exposed data is monetizeds

08.

USE CASE 5: MOBILE THREAT PROTECTION

Protecting Mobile-First Customers from Rogue Apps and Mobile-Based Fraud

As customers increasingly rely on mobile banking, attackers exploit mobile channels to distribute fake apps, repackaged applications, overlays, malicious APKs, and device-based threats. These tactics can be used to steal credentials,intercept sessions, capture sensitive information, or support account takeover.

Mobile threats are especially dangerous because customers may believe they are interacting with a legitimate app experience. Once installed or engaged, malicious mobile assets can become a direct path to data theft and account compromise.

How 360 Brand Guardian Helps

360 Brand Guardian helps institutions detect and respond to mobile-based threats targeting customers and digital channels

Business Value

Mobile Threat Protection helps safeguard mobile-first customers, reduce credential theft risk, protect the institution's digital experience, and prevent rogue apps from becoming an entry point into broader fraud activity.

COMMON THREAT SCENARIOS

- Fake banking or financial apps
- Repackaged or tampered mobile applications
- Overlay attacks designed to capture credentials
- Malicious APKs distributed outside official app stores
- Jailbroken, rooted, emulator-based, or risky device environments
- Pharming and man-in-the-middle attacks

THE SOLUTION HELPS INSTITUTIONS:

- Identify fraudulent and malicious mobile apps across official and unofficial sourcesl
- Detect repackaged apps, overlay attacks, and risky mobile attributes
- Support remediation and removal of high-risk mobile assets
- Provide intelligence to fraud and security teams
- Reduce customer exposure to mobile credential theft and account takeove

09.

USE CASE 6: AI-GENERATED SCAM DISRUPTION

Disrupting Scams That Scale Faster Than Manual Response

Generative AI has made scams more scalable, convincing, and difficult to detect manually. Attackers can use AI to create realistic phishing messages, malicious ads, spoofed emails, fake support content, scam landing pages, and social engineering campaigns.

For financial institutions, this creates a speed and scale challenge. Scam infrastructure can change quickly, produce multiple variants, and move across email, web, social, mobile, and advertising channels.

How 360 Brand Guardian Helps

360 Brand Guardian helps institutions detect and disrupt AI-amplified scam activity across digital channels.

Business Value

AI-Generated Scam Disruption helps institutions detect fast-moving scam campaigns earlier, reduce exposure two phishing and malware, protect brand trust, and respond faster to threats that move across multiple digital channels.

COMMON THREAT SCENARIOS

- AI-generated phishing pages and messages
- Spoofed emails and forged sender identities
- Malicious ads redirecting users to phishing or malware
- Fake invoices and BEC-style scams
- Malware hidden in files, unofficial apps, or deceptive downloads
- Rapidly changing scam landing pages

THE SOLUTION HELPS INSTITUTIONS:

- Detect phishing, malware, spoofing, and malvertising before customer impact
- Identify spoofed domains and forged sender identities
- Monitor advertising ecosystems for malicious contents
- Detect malicious mobile apps and phishing-related malwares
- Correlate scam infrastructure across web, email, mobile, advertising, and social channels
- Support takedown actions to remove harmful assets

10.

THE GUARDIAN FUSION CENTER

AI and Human Expertise for 24/7 External Threat Response

360 Brand Guardian is strengthened by the Guardian Fusion Center, a 24/7 operation that combines AI-powered monitoring with experienced threat analysts. This model helps institutions filter noise, prioritize the most impactful threats, and act quickly when malicious assets target the brand or customers.

The Guardian Fusion Center supports institutions by:

- Continuously monitoring for external threats
- Investigating and validating high-risk findings
- Supporting takedown and deactivation workflows
- Reducing the need for internal teams to manually manage every threat
- Providing intelligence and reporting for fraud, security, and business stakeholders

HOW 360 BRAND GUARDIAN WORKS

1 DETECT

24x7 monitoring across web, social, mobile, domains, and underground channels

2 ANALYZE

Correlates signals, validates threats, and prioritizes severity

3 DISRUPT

Takes down sites, profiles, apps, ads, and malicious infrastructure

4 COORDINATE

Shares evidence with fraud, security, legal, and compliance teams

5 REDUCE RISK

Protects customers, preserves trust, and lowers fraud exposure

For financial institutions with limited fraud, security, or brand protection resources, this expert-led model can function as an extension of the internal team.

Proof Points and Metrics

360 Brand Guardian supports measurable outcomes across external threat management, fraud prevention, and operational efficiency.

Operational Value Areas

360 Brand Guardian helps financial institutions strengthen external threat management by giving fraud, security, marketing, legal, and customer protection teams better visibility into threats that emerge outside owned digital channels.

Instead of relying only on customer reports or manual searches, institutions can use 360 Brand Guardian to support a more proactive and coordinated approach across key operational areas:

- External threat visibility: Identify phishing, smishing, spoofed domains, fake websites, rogue apps, impersonation profiles, malicious ads, and exposed data across public and underground channels.
- Threat validation and prioritization: Help teams focus on higher-risk findings by analyzing context, behavior, threat indicators, and potential customer impact.
- Takedown and disruption support: Support coordinated action against malicious assets across hosting providers, app stores, social platforms, domain registrars, and other external ecosystems.
- Cross-functional collaboration: Provide shared intelligence and evidence for fraud, security, marketing, legal, compliance, and executive stakeholders.
- Operational efficiency: Reduce dependence on fragmented manual processes by centralizing external threat monitoring, investigation, escalation, and reporting workflows.
- Customer and brand protection: Help limit customer exposure to scams that misuse the institution's brand, digital presence, executives, employees, or customer-facing channels.

Operational Value in Action

- 83% global proactivity rate
- More than 116,000 threats deactivated in 2024
- More than 890 threats deactivated per client in 2024
- 24/7 proactive monitoring and support through the Guardian Fusion Center
- Coordinated disruption workflows designed to reduce customer exposure while takedown or deactivation actions are in progress

11.

CUSTOMER PROOF POINTS

Trax Credit Union

Trax Credit Union needed a simple solution to proactively monitor phishing emails directing members to fake websites. With 360 Brand Guardian, Trax implemented proactive monitoring and takedown of phishing and fake websites. The solution was transparent to members and employees, reduced internal workload, and provided proactive reporting and 24x7x365 support.

FNB Hutchinson

FNB Hutchinson used 360 Fraud Protection to respond to real-world external threat scenarios, including CEO impersonation, smishing attacks, and Debit Card BIN exposure. The bank was able to escalate threats, receive updates, and take proactive action to reduce customer and cardholder risk.

Progressive Bank

Progressive Bank faced counterfeit websites and phishing attempts targeting its customers. With 360 Brand Guardian, the bank proactively monitored and removed counterfeit and phishing websites, while multiple unauthorized mobile applications were identified and removed without involvement from the bank's internal team.

Banco Galicia

Banco Galicia implemented 360 Brand Guardian to monitor and dismantle counterfeit and phishing websites. The solution helped the bank protect digital channels from external threats while supporting a secure and seamless banking experience for more than 3.8 million customers.

Conclusion

Financial institutions cannot protect customer trust by waiting for fraud to reach the login screen or transaction flow. By then, attackers may have already abused the brand, deceived the customer, harvested credentials, or exposed sensitive data.

360 Brand Guardian helps institutions move earlier in the fraud chain. It detects, monitors, and deactivates external threats across phishing, smishing, brand abuse, impersonation, mobile threats, malvertising, spoofing, malware, and deep and dark web exposure.

With continuous monitoring, AI-powered intelligence, expert-led support from the Guardian Fusion Center, and coordinated takedown workflows, 360 Brand Guardian helps financial institutions reduce customer exposure, lower operational burden, protect brand trust, and disrupt scams before they cause harm.

READY TO PROTECT YOUR BRAND AND STOP SCAMMERS BEFORE THEY REACH YOUR CUSTOMERS? **GET A DEMO.**

AppGate helps organizations protect their customers, digital channels and brand reputation from evolving cyber and fraud threats. With 360 Fraud Protection, AppGate enables financial institutions to detect and mitigate external threats, reduce fraud risk and strengthen trust across the digital customer journey. The 360 Fraud Protection platform includes 360 Brand Guardian, 360 Risk Control and 360 Adaptive Authentication, helping organizations identify threats earlier, take action faster and protect customers before fraud can escalate. Learn more at 360fraud.ai.

360 fraud protection
by AppGate

©2026 AppGate. All Rights Reserved. The AppGate logo and certain product names are the property of AppGate. All other marks are the property of their respective owners. SAC-3537