BRAND ABUSE MITIGATION SERVICE

Evolving Fraud Landscape

With financial institutions facing increasingly evolving threats such as unauthorized or malicious online brand and intellectual property use, rapid response is vital. Employing advanced tools and expertise, ThreatMark's **Cyber Fraud Fusion Center** offers comprehensive protection against phishing attacks and brand abuse, reinforcing the overall security posture of businesses in the digital landscape.

ThreatMark's Distinct Capabilities

Globally, financial institutions face increased levels of malicious online use of their brand and intellectual property. This unauthorized usage results in online fraud, revenue loss, damage to the brand's reputation when customers encounter scams, legal risks from not actively defending trademarks, and dilution of brand identity from inconsistent presentation.

ThreatMark's Brand Abuse Mitigation Service works with ISPs and social platforms to eliminate infringing content and take down counterfeit sites. It also allows reporting each site to ThreatMark for an in-depth investigation and site takedown.

Swift Action on Suspicious Sites

Every site using a client's branded content or logo is immediately investigated by our expert fraud analysts for potential trademark infringement.

In-Depth Investigation Tools

- Domain Owner & Registrar Indentification through WHOIS and GeoIP.
- Hosting Provider Indentification.

Meticulous Documentation

Detailed evidence capturing:

- Owner Details
- Compromised Site Date
- Screenshots
- URLs

Mitigation for Significant Breaches

- Alert the insitution of sever findings.
- Notifications to:
  - Content Providers
  - Brand Owners
  - Partner Orgganizations
- Targeted URL Takedown

DISRUPT FRAUD, GAIN TRUST.

How ThreatMark can Support Financial Institutions

ThreatMark's Cyber Fraud Fusion Center offers organizations an additional cybersecurity service with streamlined operations and a robust defense against phishing and malware, reducing potential financial losses. Through key digital partnerships, we ensure swift threat mitigation with minimal disruptions, optimizing response times to fraudulent activities. Our services enhance return on security investments and proactively hunt threats, safeguarding assets and reputation.

- **Reduced Fraud Costs**
  Expert tools and tactics directly combat phishing and malware, curtailing potential financial losses.
- **Operational Efficiency**
  Quick threat mitigation, due to relationships with key providers, minimizes disruptions and response times.
- **Enhanced Security ROI**
  Maximize the return on security investments by providing an all-encompassing defense.
- **Risk Management**
  Proactive threat hunting reduces unforeseen vulnerabilities, safeguarding assets and reputation.

Advanced Defense

- Integrations with hosting, registrators, and ISVs.
- Cutting-edge technology for multi-channel detection.
- Ensures enhanced detection accuracy.

Swift Response Times

- 6 seconds average time for detection to notification.
- Ensures first measures are effective within 2 hours.

Dedicated Cybersecurity Team

- Provides 24/7 response to incidents.
- Supports and guides on best practices.
- Service activated in less than 5 days.

Proactive Mitigation

- 90:10 ThreatMark Detection vs Client Detection.
- Executes both automatic and manual checks.
- Notifies relevant search engines, hosting providers, etc.

Expert Fraud Analysis

- Investigate phishing sites comprehensively.
- Assesses threat levels and severity.
- Documents findings in detail: IP, source code, etc.

Flexibility

- Adapts and learns continually from new threats.
- No major integration or investment required.
- Serves as a standalone service option.