SOLUTION BRIEF

proofpoint.

FINANCIAL SERVICES: MANAGING DIGITAL RISK AND COMPLIANCE

Brand trust and customer engagement have always been the lifeblood of financial institutions (FIs). Today, they're more critical than ever as FIs engage with customers across digital channels such as the web, social media, and mobile apps. While the mission of financial services firms hasn't changed, their risks have. FIs must comply with evolving public communications rules. And they must ensure the digital engagement doesn't introduce new security and fraud risks to their brand and customers.

Cyber criminals go anywhere there's a potential financial gain, and FIs a top target. More people are falling victim to brand fraud, account takeovers, and customer-support fraud (or "angler phishing") across social, mobile, and web channels.

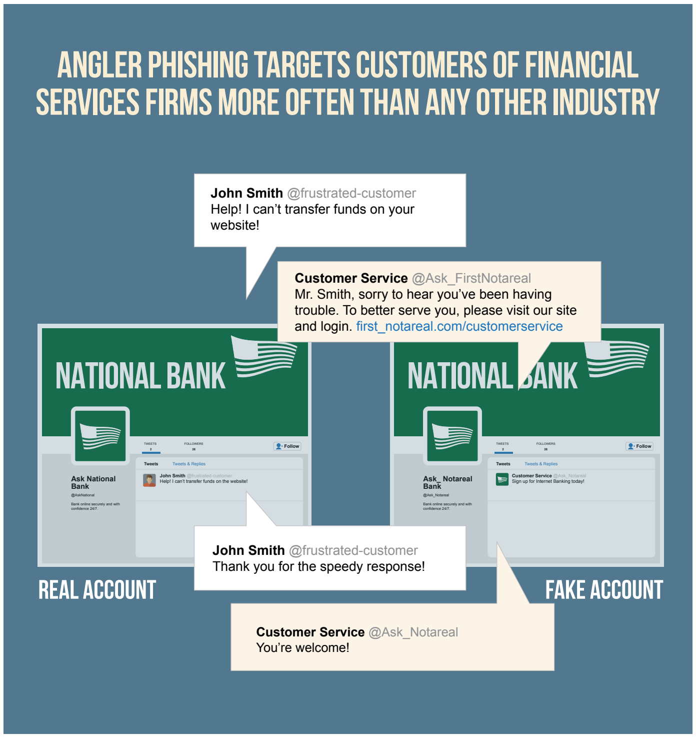
To fight back, you need a digital risk and compliance solution built for all your digital channels. Here's an overview of digital risks and compliance challenges facing FIs and what you should consider in a solution.

SOCIAL MEDIA RISKS

Branded social media accounts are a key part of modern marketing. In an American Bankers Association survey, 76% agreed or strongly agreed that social media is important to their banks. And 73% feel their bank is somewhat active to very active in social media.[1]

This focus makes social media a prime target for cyber criminals. They set up fraudulent social media accounts to masquerade as financial brands and defraud your customers.

Angler phishing targets customers of financial services firms more often than any other industry. The attacker hijacks your customer support conversations on Twitter. When a customer tries to connect to you in a tweet, the attacker responds through a lookalike social media account. From there, they obtain your customer's account credentials, security questions and answers, Social Security number, and other sensitive information. These can lead to real monetary losses, a damaged brand, and compliance violations.



ANGLER PHISHING TARGETS CUSTOMERS OF FINANCIAL SERVICES FIRMS MORE OFTEN THAN ANY OTHER INDUSTRY

John Smith @frustrated-customer
Help! I can't transfer funds on your website!

Customer Service @Ask_FirstNotareal
Mr. Smith, sorry to hear you've been having trouble. To better serve you, please visit our site and login. first_notareal.com/customerservice

John Smith @frustrated-customer
Thank you for the speedy response!

Customer Service @Ask_Notareal
You're welcome!

Solution Considerations

- Establish an automated process that continuously monitors social media for fraudulent accounts that impersonate your brand.
- Monitor messages on your community and social customer service accounts for angler phishing. Make sure the process is automated and continuous.
- Implement real-time alerts and an account takedown process.

[1] American Bankers Association. "The State of Social Media Banking." March 2017.

DOMAIN RISKS

Your firm's web presence is a lucrative target for threat actors looking to cash in on your digital investment. The volume of phishing websites climbed 250% in Q1 2016.[2]

Cyber criminals register domains that imitate your brand. Piggybacking on your brand's goodwill, they use the domain as part of a lookalike website or email to deliver credential and credit card phishing schemes.

Domain fraud leads to real financial losses—for which your firm may be liable. Phishing costs brands an estimated $4.5 billion worldwide each year.[3]

PHISHING COSTS BRANDS AN ESTIMATED $4.5 BILLION WORLDWIDE EACH YEAR

Solution Considerations

- Monitor your brand's domain presence and take down suspicious or dormant domains that pose a risk to your customers.
- Detect and quickly take down URLs that are part of active phishing campaigns.
- Enable remediation workflow through integration with takedown providers.

MOBILE APP RISKS

Many customers manage bank and financial transactions through mobile apps. In fact, 90% of FIs agree or strongly agree that in five years customers will use mobile devices as their primary source of bank communication.[4]

As a result, mobile banking apps are now fertile ground for cyber criminals. Attackers create fake apps that impersonate your bank and attack the people who trust it. More than 16,000 of app developers around the world distribute malicious apps through mainstream and third-party app stores.[5]

Today's global app store ecosystem is large and dynamic. Failing to keep track of your mobile presence or stop fraudulent or unsanctioned brand apps could be costly. To safeguard your brand and protect customers, you need to constantly monitor for mobile app risks. And when you find them, you need the right procedures, tools, and policy to take them down quickly.

Solution Considerations

- Establish an automated process to monitor mobile apps stores for fraudulent apps that may try to steal your customer's credentials.
- Adopt built-in workflows that enable prompt takedown of infringing and rogue apps.

DIGITAL COMPLIANCE

The average brand has 320 social media accounts. With so many accounts, corporate governance and compliance can get complex. Reign in account sprawl and supervise your digital content. Ensure it all complies with public-communications and retention rules from FINRA, SEC, FCA, IIROC, and others.

This task might sound like a resource drain. But engaging on digital channels while ensuring compliance doesn't have to be a headache. Here's how to simplify your efforts.

90% OF FINANCIAL INSTITUTIONS WILL USE MOBILE DEVICES AS THEIR PRIMARY SOURCE OF BANK COMMUNICATION IN FIVE YEARS.

Solution Considerations

- Automate account discovery, content monitoring, and content supervision.
- Apply content controls that automate content remediation.
- Adopt a flexible solution that lets you hand off content retention to your in-house archiving solution or has built-in archiving.

[2] Anti-Phishing Working Group. "Phishing Activity Trends Report 1st Quarter 2016." May 2016.
[3] Finance Digest. "3 Top Digital Asset Threats Facing Your Brand in 2017." February 2017.
[4] ABA. "The State of Social Media Banking." March, 2017.
[5] Proofpoint. "Mobile Malware Masquerades as POS Management App." March 2017

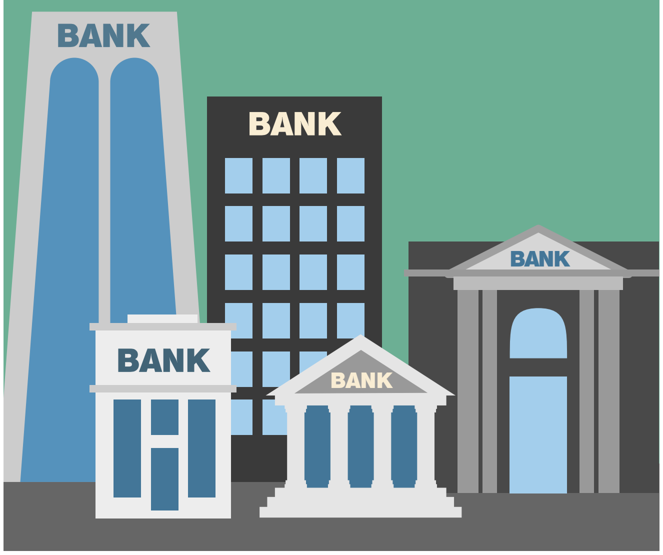
MANAGE DIGITAL RISK AND COMPLIANCE WITH PROOFPOINT

At Proofpoint, we know the value of enabling positive digital engagement and protecting your customers and brand. We also understand the constant state of change FIs face in digital engagement channels. That's why we nurture the largest partner ecosystem. We make it easy to integrate our digital compliance and security technology with the digital-enablement technologies you already use.

Our platform is a unified solution to protect against security, brand, and compliance risks across web, mobile, and social media. It's the only solution that gives you a holistic defense for all your digital engagement channels.

Proofpoint Digital Risk Defense automatically discovers and monitors your digital attack surface on social media, mobile apps, and the web. When we detect activity that poses a security risk, our automated remediation and takedown services help you stop it right away.

5 OF THE TOP U.S. BANKS USE PROOFPOINT



We also simplify your compliance efforts. We offer the industry's only end-to-end social media compliance solution. You can discover and track all assets across all digital channels. You can also automatically supervise, remediate, and archive content. We help ensure that your engagement meets public-communications and retention requirements for financial services. With Digital Risk Defense, you can:

- Prevent and remediate all misleading, material connections, or bias in communications.
- Get demonstrable proof of policy and enforcement. Apply policy for your industry and regulations, including FINRA, SEC, FCA, FTC, and others in minutes.
- Automatically scan content across all your social media properties. Get alerts right away and even remove the content when a violation is detected.
- Automatically hand off social media content to your in-house archive or to our solution's built-in archiving.

No other solution makes it easier for FIs to safely engage on digital channels and stay compliant.

LEARN MORE

To learn more about Proofpoint Digital Risk Defense visit: proofpoint.com/digital-risk

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.