proofpoint.

SOLUTION BRIEF

Securing Financial Services and Insurance Organizations with Proofpoint

Protecting People, Financial Data and Assets

PRODUCTS

- Proofpoint Email Security and Protection
- Proofpoint Security Awareness Training
- Proofpoint Browser Isolation
- Proofpoint Meta
- Proofpoint CASB
- Proofpoint Compliance and Archiving Solutions
- Proofpoint Data Loss Prevention Solution
- Proofpoint Insider Threat Management

KEY BENEFITS

- Protect against email fraud
- Keep employees educated about cyber risks
- Archive data and stay compliant
- Prevent data loss

The pandemic has forced many Financial Services and Insurance (FSI) firms to accelerate its digitalization efforts. Notably, to ease everyday customer journeys remotely and ensure new virtualized communication and compliance needs. These accelerated infrastructure changes have also expanded FSI firms' user perimeter.

The changes have helped bankers, wealth advisors and traders manage markets and financial flows. But it has also offered more opportunities for threat actors. Proofpoint can help mitigate these risks. Our cybersecurity and compliance solutions protect you, your organization and your customers.

Keeping Up with a Changing Threat Landscape

FSI firms are the largest target for threat actors amongst all industries. In addition to the traditional TTPs of social engineering and business email compromise (BEC), the pandemic has seen a rise in exploiting stimulus measures and financial aid programs.

Our researchers have found that the cumulative volume of coronavirus-related email lures now represents the greatest collection of attack types united by a single theme.

These attacks, all leveraging coronavirus lures, span across:

- Credential phishing
- Malicious attachments
- Malicious links
- BEC
- Fake landing pages
- Downloaders
- Spam
- Malware

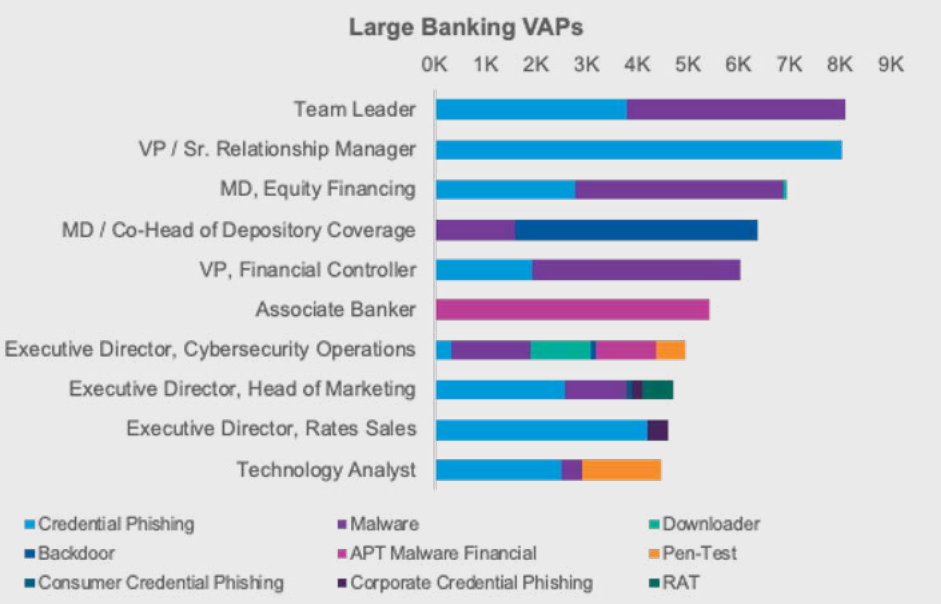


Figure 1: Breakdown of Very Attacked People at a leading Commercial Bank.

As threat actors seek new ways to infiltrate an FSI firm, it has made every person in your firm represent a different security level or compliance risk.

For example:

- Bank lending or insurance underwriting groups can access individual and business financial information as well as personally identifiable information (PII)
- Investment bankers and asset managers have access to market-moving and non-public information, which significantly raises their vulnerability level
- Traders regularly interact with various ecosystem firms (buy-side and exchanges) which increases supply chain risk and utilize sought after proprietary trading models

Take a People-Centric Approach

Security practitioners prioritize defenses against the most vulnerable technological attack surfaces. Yet when it comes to addressing the human attack surface, we still apply broad strokes of protection. Firms need to be as focused on a people-centric security approach that rivals the level of detail that threat actors engage in.

FSI firms need to protect their industry with security through:

- Education
- Role-based entitlements
- Data loss prevention
- Data lifecycle management
- Zero-trust asset protection

Our 2020 report, "Financial Services and Insurance Industry Threat Landscape" explores what we call Very Attacked People™ (VAPs) in FSI industry. They are users within an organization who are the most heavily targeted by cyber threats. Figure 1 shows a real-life commercial banking example.

Here the team leader and relationship manager were the most attacked titles. Both are sales roles in the bank's loan group. And they are subject to stiff compliance requirements and consumer protection laws. They require adequate monitoring and audit trails. Lenders will see various attacks because threat actors have ample opportunities to gain sensitive information across a loan's lifecycle to gain sensitive information.

For example, PII or account takeover. Also, lenders are exposed to supply chain risk because they use different third-party systems and partners. They help them facilitate a loan's origination, underwriting and closing.The attacker here pretended to be an office admin and sent emails regarding document verification. Knowing the VAP helped isolate the problem. And appropriate security measures were directed.

Financial Services Use Cases—How Proofpoint Can Help

Secure and compliant customer engagement

Proofpoint Digital Risk Protection secures your brand and customers against digital security risks across web domains, social media and the dark web. It gives your FSI firm a holistic defense for all your digital engagement channels. For example:

- **Social Media Protection:** Secure your company and customers from digital risks for your entire social media infrastructure. We protect your social media presence from account takeovers, social media phishing scams and malicious content.
- **Social Media Compliance:** Modern compliance and governance requirements include regulation for social media. Bridging the gap between social media compliance and marketing practice can be a big challenge. Monitor and remediate on social media in real time at scale.
- **Content Capture and Patrol:** Capture all your communications in a single platform for regulatory compliance and data management that ensures you are capturing the full fidelity of over 25 new and most popular communications channels.
- **Web Domain Fraud Monitoring:** Protect your domain investments from domain squatters, typo phishing campaigns and other infringing domains. Our digital protection solution applies artificial intelligence to uncover fraudulent domains that pose a risk to your brand and customers. We also safeguard your brand-owned domains by letting you know if your domain registrations or SSL certificates are about to expire.

Secure employee and partner communication and collaboration

FSI firms encompass a wide range of groups and IT environments coordinating, collaborating and sharing information between front, middle and back offices. Email is a popular method of disseminating confidential information, and a large majority of high-profile FSI data breaches begin with targeted phishing attacks. We have the right solutions for the FSI industry by protecting users in the way they work today:

- **Email Protection** delivers top-rated email security to stop malware and non-malware threats.
- **Data Loss Prevention (DLP)** mitigates the risk of email data loss and protects against email fraud.
- **Browser Isolation** allows your users to browse the web while preventing malicious content from impacting your corporate devices.
- **Meta,** a zero-trust solution, quickly and securely connects employees, partners and customers to your datacenter and cloud. You get tighter security, a far better user experience and reduced IT hassle. Secure financial communication and collaboration.

Protection against impostor attacks

Impostor emails are fraudulent messages designed to look like it's from someone the recipient knows or can trust. These attacks can be hard to detect because they don't exploit technical vulnerabilities. They target specific job functions like HR, IT and finance, that have access to monetizable activity. For FSI this is also typically seen in front-office roles. For example, brokers, investment bankers, advisors and financial sales agents as well as operations and back-office roles.

We offer an integrated, people-centric, end-to-end solution. It stops all forms of email fraud, no matter the tactic used, or the person being targeted:

- **Advanced Email Security** blocks phishing and impostor emails that use spoofed and use lookalike domain names. It uses advanced machine learning and multiple detection engines to detect these targeted attacks. And it stops them before they reach users' inboxes.
- **Domain-based Message Authentication Reporting and Conformance (DMARC)** is deployed to help email authentication. It stops spoofed email before defrauding employees, clinical staff and business associates.

Securing Microsoft 365 and other cloud environments

FSI firms have accelerated their efforts to move data and applications to the cloud. And they are accessing more sensitive data over internet connections. They need to see cloud activity as it unfolds across the FSI ecosystem and supply chain. A cloud access security broker (CASB) is a critical element of cloud security architecture.

Proofpoint CASB helps organizations:

- Scan and act quickly on potential cloud-based email policy violations
- It reduces the risk of a cyber-attack or data breach
- It uses an organization's email flow to identify confidential data within cloud file services including Microsoft 365, DropBox, Box and Salesforce

Insider threat protection

Insider threats affect multiple assets—data, devices, workloads, networks and people—and the impacts can be acute or broad in scope. The most common insider threat risks and data loss for FSIs include:

- Theft of the intellectual property, loss of operations, affectations of brand
- Financial Fraud: wire transfers, securities fraud, money laundering, market manipulation
- Sensitive Data: PII, PCI, PHI

Proofpoint Insider Threat Management (ITM) protects against data loss, malicious acts and brand damage. It involves insiders acting maliciously, negligently or unknowingly. Our ITM solution correlates activity and data movement. It empowers security teams to identify user risk, detect and respond to insider-led data breaches. And it accelerates security incident response.

Key capabilities for FSI firms are:

- Handling of Sensitive Data: Quickly identify risky user activity and data movement (e.g., DSS4, Red Flags Rules, GDPR)
- Ability to Prevent Breaches: Guardrails in place to protect data breach and service disruption (e.g., Reg S-P, FACTA, SWIFT)
- Ability to Respond: Capability to rapidly mitigate damage from threats (31 CFR Ch. X)
- Auditability: The ability to respond to audits efficiently (GLBA, Dodd-Frank)

Keeping critical financial, trade, PII, client and intellectual property information safe

Having the right email data loss prevention (DLP) ensures sensitive and critical information is classified and accessed by the right people.

With **Proofpoint People-Centric DLP**, FSI firms can:

- Identify and respond quickly to data risks posed by negligent, compromised and malicious users
- Define data of interest and leverage these definitions across the entire platform
- Protect the confidentiality of individual email messages through **Email Encryption**
- Allow the user community to trigger encrypted messages automatically by adding a keyword of choice to the subject line, or trigger message-level encryption on the basis of DLP rules

Manage regulatory compliance standards while reducing complexity

FSI firms are highly regulated. It requires greater financial customer data transparency and transaction protections. The new evolving hybrid work environment and digital customer engagement adds to the complexity. It requires a scalable, agile and intelligent compliance platform to match. Proofpoint Archiving and Compliance solution provides all-in- one people-centric compliance.

- **Intelligent Supervision:** Meet supervision requirements for email and other communications. Reduce "noise" by ignoring pre-approved content, skipping low-risk content (like bulk mail) and threading conversations. Your compliance team can find violations faster and more accurately.
- **Enterprise Archive:** Securely archive data in our grid-based cloud storage infrastructure. High-performance near real time search greatly reduces the time and cost of collecting and exporting information for e-discovery or audit purposes.
- **E-Discovery Analytics:** Dashboards and visualizations help identify patterns worth investigating. Topic clustering and timeline graphing enables you to define your search criteria more precisely.
- **Compliance Gateway:** Ensure that content is properly retained. It has a built-in feedback loop to confirm that the archive successfully processed each message from your content sources.

Raising FSI user security IQ

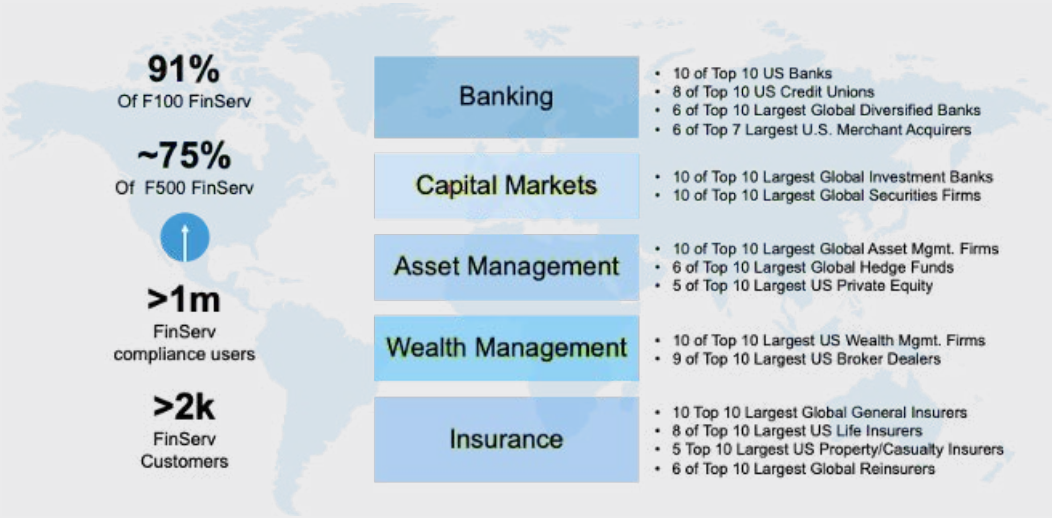
Improving education to make employees more aware of what to look for in their dealings can have a major impact in prevention. Security can be improved to have a more holistic operational risk awareness program.

- **Proofpoint Security Awareness Training** provides employees training to spot healthcare-themed social engineering attacks, such as sophisticated phishing ploys.

Actionable and embedded security intelligence

Your workforce needs to use on-premises systems and cloud applications securely, regardless of where they connect from. To deploy a security program focused on people, you need the right visibility, controls and integrations.

- **Proofpoint Nexus People-Risk Explorer:** Unified view of your people-centric security risk across the Proofpoint suite and third-party products.
- **Targeted Attack Protection (TAP)** helps you stay ahead of attackers with an innovative approach that detects, analyzes and blocks advanced threats before they reach your inbox.
- **Proofpoint Threat Response** shares intelligence on new threats that enables security teams to respond faster and more efficiently to the everchanging threat landscape.



Visibility for your Greatest Cybersecurity Risk: Your People

Our solutions protect clients, employees and third parties at more than 90 of the Financial Services Fortune 100 companies. We offer the industry's leading end-to-end people-centric security solution that changes and secures how you communicate, collaborate and comply.

LEARN MORE

For more information, visit https://www.proofpoint.com/us/solutions/financial-services-and-insurance.