ZeroFOX recorded a 56% annual increase in digital threat activity targeting the financial services sector. As financial institutions continue to engage with customers digitally, they must equip themselves to handle the sophistication and scale of threats they will encounter.
Executive Summary

For financial services (FinServ) institutions, digital engagement means business. Financial customers expect to digitally engage with financial organizations through online portals, social media support, and mobile apps. FinServ institutions are adopting these platforms to compete for customers and maintain high levels of satisfaction. However, financial organizations are not the only ones that recognize the value of digital platforms. As FinServ organizations continue to engage with customers digitally, they must equip themselves to handle both the sophistication and scale of threats they will encounter on these platforms. Cybercriminals capitalize on this new and expanding attack surface, relying on fraudulent mobile applications, spoofed domains, and impersonating accounts to engage with financial customers in the same way they would engage with their legitimate financial service provider. To carry out these various attacks, criminals exploit the no-cost social landscape, low technical barriers, ease of target acquisition and payload delivery, and broad access to potential victims that these platforms provide. The goals of these actors are familiar and mostly financially motivated. Through impersonation and fraud, attackers gain access to financial customers, their information and their money, leveraging the trust and brand financial institutions have worked so hard to build online.

This report provides a comprehensive review of the digital threat landscape facing the financial services industry, with a focus on the top tactics cybercriminals used to plan and execute attacks on financial institutions and their customers. Findings are based on threat data collected across ZeroFOX's FinServ ecosystem, including banks, brokerages, cryptocurrency exchanges, credit unions, credit reporting agencies, insurance providers, and investment firms over the course of 12 months. Data was analyzed across protected assets, including threats targeting company executives, domains, products, employees, customers, brands, and other owned assets, as well as non-owned assets that were used to impersonate the institution, brands and executives. This included analysis across a comprehensive set of data sources, inclusive of social media, surface web, deep and dark web, mobile app stores, market places, and many other digital platforms that ZeroFOX monitors. For this report, the ZeroFOX Alpha Team analyzed and enumerated the threat actor tactics regularly observed across these platforms, providing insights into how common the various tactics are being used against the financial services sector and recommendations for how FinServ organizations can protect themselves from these threats.

Key Findings

Financial Services Digital Threat Activity Grew 56% Year over Year

Across ZeroFOX's customer ecosystem, the financial services industry is in the top 3 most targeted industries for digital attacks. Further, FinServ security events increased 56% from the previous year, and takedowns (e.g., the removal of spurious content from social media posts and threads or removal of imposter domains and accounts) increased 188% year over year.

Brands Incur Abuse and Manipulation Activity on Average 2-3 Times Daily

This category of attack activity was the most popular, generating over 250,000 detected events. While 90% of these events were name impersonations, many are not easily detected due to advanced disguising techniques attackers utilize.

System and Information Exploitation Grew 26% within the Past Year

Attackers are increasingly adept at compromising systems, and social media has increasingly become the conduit. They also blatantly market their heists both publicly and privately, across all digital channels. Malicious domains top the list of attack techniques at 57% share, with another 18% coming from information disclosures found on paste sites, most of which are accessible to the public.

FinServ Organizations Endure almost 3 Takeover Attempts per Month

Corporate social media account takeover attempts occur nearly 30 times per year on average for every institution (nearly 3 per month). Additionally, on average 4 credential compromises (of which 2.3 originate from breach databases) occur per executive annually, which often lead to takeover or impersonation. Each FinServ organization has on average 30 targeted executives.

75% of Financial Fraud and Scams Occur on Mobile Apps and Social Media

Fraud accounted for 40% of all digital attack activity against financial services organizations and their customers. In total, there were over 87,900 unique financial fraud scams observed. Of these, 37% were money-flipping scams, 28% were customer giveaway/coupon scams, and 27% were crypto-currency related scams. Rogue Mobile Apps accounted for a portion as well - there were 489 fake mobile app incidents identified during the period.
Table of Contents

The Financial Services Digital Landscape ................................................................. 1
  Financial organizations and their customers connect digitally ................................. 1
  Attackers seize the opportunity and have near equal customer access ...................... 1
  Anatomy of a digital attack ..................................................................................... 2

Attack Tactics Targeting Financial Institutions ......................................................... 3
  System and information exploitation ....................................................................... 4
  Brand abuse and manipulation .................................................................................... 5
    Case Study | Malicious Mobile App: Banking Trojan .............................................. 6
  Account takeover ........................................................................................................ 7
  Fraud and scams .......................................................................................................... 8
    Case Study | Check Forging Scam ........................................................................... 9

Conclusion & Recommendations .................................................................................. 10

Methodology .................................................................................................................. 11

Sources ............................................................................................................................ 12
The Financial Services Digital Landscape

Financial organizations and their customers connect digitally

Nowhere is the digital revolution more apparent than in financial services. Today, financial institutions rely on social and digital platforms to promote product offerings, recruit customers, provide services, and engage in customer support activities. Online banking platforms allow clients to easily manage their money, expedite account transfers, secure loans, and execute many other transactions. Online financial services entities, such as e-brokerages or e-insurers, similarly sell products and services, allowing customers to transact business and make purchases easily. Brand and marketing teams rely on social media and digital advertising to enter new markets, generate awareness, and connect with potential customers. Customer support teams engage with customers through mobile apps and provide real-time support through social channels. The engagement between financial customers and their FinServ institutions involves sensitive information, including account credentials, credit card numbers and PII, or personally identifiable information, making this digital landscape a prime territory for cybercriminals to operate.

Attackers seize the opportunity and have near equal customer access

Understanding cybercrime, and how attackers operate, is crucial to digital risk reduction. Cybercriminals flock to both the surface and dark web, messaging groups, and even social media to market their portfolios of tools, including attack infrastructure and malware, and to dump data, sell stolen financial information, and network with other criminals. Closed dark web forums provide an outlet for attack planning and monetization - in the form of selling information and hacking-as-a-service capabilities. Threat actors use social media to connect and collaborate with each other, just like the rest of us. Criminal groups on social media platforms allow actors to network, promote their services, and even boast about previous attacks. Domains and the email addresses derived from them are used as staging grounds to host a web or mail server in order to impersonate legitimate brands to conduct attacks.

Telemetry collection and analysis is key for fraud detection, digital fingerprinting, incident response, and threat intelligence. Telemetry is more than what an institution knows about asset usage inside its perimeter; it also includes signals that derive from sources outside of an institution's own environment which they do not own. While a financial institution may not control all the assets in their service-delivery chain, their customers expect to be safeguarded by the financial organization when accessing their applications and platforms. For instance, banking customers are not part of the typical financial institution's endpoint and mobile device management policies. These customers do not use the same email systems employed by the organization, and may not be educated with regards to popular phishing scams and other email security concerns. As customers engage with FinServ organizations on these platforms, bad actors attempt to engage with them.

In the modern digital world, financial services organizations must realize that their customers operate in a contested environment and that cybercriminals are the same ‘distance’ to customers as the financial institutions themselves.

This places an added burden on financial institutions to protect their current and prospective customers.
Anatomy of a digital attack

While attack tactics vary by vector of attack, most digital attacks (those emanating from outside the organization’s firewall) follow a similar pattern as follows:

1. The attacker works to obtain credentials or identities of accounts or personnel belonging to the organization. This can be via means such as acquiring spilled usernames and passwords from a website breach or password dump site, from social engineering, from spear phishing attack targeting select high-profile individuals, etc.

2a. Once credentials are obtained, the attacker may attempt infiltration of corporate networks to access employee or customer databases. They may also use an account checker to test the stolen credentials against many websites (for instance, social media sites or online marketplaces). Additionally, the attacker may attempt a takeover of the organization’s social media account(s) or domain pages. Direct account access of social media account takeovers are preferred by attackers, since it is an easier path to gain desired data, funds, or customer access.

2b. If direct access isn’t possible, the attacker may impersonate the financial institution’s top executives or brand via spoofed accounts/pages. This method relies on recognition and trust to lure prospects and trick customers into thinking they are dealing with the legitimate institution.

3. The attacker, acting as an imposter misusing the financial institution’s brand or executive identity, casts a wide net to lure prospects and customers. Ultimately, some users fall prey to this trickery and divulge sensitive account details (user logins/passwords) or are scammed into revealing credit card numbers, PII, etc.

4. The attacker drains stolen accounts of stored value, credit card numbers, and other personally identifiable information and quickly monetizes their attack spoils.

5. The attacker may also use account information going forward for other nefarious purposes (for example, to send spam, sell the information on black marketplaces, or create further transactions).

Digital Attack Flow

Digital attacks emanating from outside the firewall follow a similar pattern.

© 2019 ZeroFOX Inc. All rights reserved. All other trademarks are property of their respective owners.
Attack Tactics Targeting Financial Institutions

We have grouped attack tactics into four main categories that this report explores, including system and information exploitation, brand abuse and manipulation, account takeover, and financial fraud and scams.

**System and information exploitation**

System exploitation is access gained to a computer system, either logically or physically, without permission. This is typically driven by what are thought of as traditional attack methods - generally, exploitation of vulnerabilities within the hardware or software of the system. These vulnerabilities may be known and unpatched, or may be 0-day vulnerabilities, which are not known to the security community but are actively being exploited by attackers. Similarly, malware and phishing attacks may also be used to gain system access and exploit information. Gaining this level of access is a primary goal of cybercriminals. Once obtained, cybercriminals have complete control over the compromised systems and the valuable information they contain, enabling multiple monetization paths.

**Brand abuse and manipulation**

Organizations make substantial investments, in both time and financial resources, to build and maintain their reputation online. Brand abuse is any form of attacker activity that seeks to take advantage of this reputation, whether it be in the form of impersonation attacks or domain spoofing. By piggy-backing on the reputation and reach of a financial service organization, attackers are able to give their malicious activity an aura of legitimacy and awareness that it would not otherwise have. The tactics used here are often conducted beyond the visibility provided by an organization’s existing security stack – which provides protection and defense-in-depth around “owned” assets, rather than fake/impersonating assets that can exist anywhere across the digital landscape.

**Account takeover**

Account takeover is the hijacking of a social media account owned by an institution, its employees, or its customers, with the purpose of gaining access and control of the account. This is done after successfully gaining access to account credentials via some other means, such as a phishing attack, information-stealing malware, active exploitation of an organization’s systems, or with credential stuffing as a result of a data breach or password reuse. Account credentials are often bought and sold on criminal forums, and hijacked accounts are often used for quick operationalization and deployment of malware, phishing campaigns, and scams. Taking over an account benefits the attacker by giving instant access to a ready pool of followers — all potential targets. Targets can then be easily and quickly exploited with fake account verification messages or other false offers which gives attackers an abundance of credentials and account details to further monetize either through their resale or direct account pilferage.

**Fraud and scams**

Financial fraud and scams intentionally deceive a victim to unlawfully steal their money or information. The latter may be information that is of value to the scammer, whether it be banking credentials, account details, or personally identifiable information. Scammers prey on the trust inherent in the victim’s relationship with the institution, and pose enticing propositions where a victim can earn money, gift cards, or cryptocurrency quickly. Scammers go to great lengths to look credible and may leverage fame or notoriety, take over an organization’s legitimate brand account, or fraudulently earn a “verified” check mark on a social media platform, in order to legitimize their efforts.
System and information exploitation

Unauthorized access to computer systems within a financial organization is attractive to cybercriminals. System access is then leveraged to steal confidential information, whether it be login credentials for online banking customers, company secrets, or some other valuable information. Additionally, an attacker could use this access to render a company's networks completely unusable, costing the affected organization millions. This was the case with the notorious WannaCry attacks, where the total cost to victims has been estimated at up to 4 billion dollars.\(^1\) This is typically achieved by traditional techniques, such as hardware or software exploits against the system, or by the use of information-stealing malware like remote access trojans (RATs) or backdoors. Increasingly, however, attackers are leveraging platforms outside of the traditional security perimeter to achieve this goal.

ZeroFOX identified 998 system and information exploitation events per FinServ organization monitored versus 743 previously — a 26% increase from the previous year; on average 255 more security events related to information exposure for each protected organization.

System and information exploitation research findings

For this category, we detected 85,880 unique events related to our financial service customers in the one-year timeframe of this study. Of these security events, 21.8% of them were deemed critical, confirmed malicious by our security operations team, and escalated to the customer. Nearly 1 in 5 of these critical security events resulted in the removal of the content in question by the ZeroFOX takedown team.

Information Exposure Security Events

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>57%</td>
<td>Malicious Domains</td>
</tr>
<tr>
<td>18%</td>
<td>Sensitive Info Paste Sites</td>
</tr>
<tr>
<td>15%</td>
<td>Attack Chatter</td>
</tr>
<tr>
<td>8%</td>
<td>Malicious Links</td>
</tr>
</tbody>
</table>

Malicious domains

Of all security events related to unauthorized access, 57% were related to impersonating domains. 79% of these fake domain-related events were on live malicious domains, which means that they were either actively serving some kind of content via HTTP, or had a mail server associated with them. These sites are often used to host additional malware, malware command and control traffic, or some other nefarious content. The mail servers can be used to send spam or phishing campaigns, or engage in other malicious email attacks.

Attack chatter

15% of these security alerts were related to “cyber attack chatter,” or discussion of attacks against FinServ institutions and their customers on social media platforms, hacking forums, or the dark web. Monitoring cyber chatter on these platforms is valuable for organizations seeking early warning, especially for the FinServ vertical. Cyber criminals may discuss new attack techniques, newly developed malware, or successfully breached organizations. This intel can also be used to inform cybersecurity organizations on current threats and what must be done to bolster defenses like prioritizing patching efforts or looking for specific attack indicators. By monitoring these sources and this kind of chatter, organizations can stay ahead of new attack techniques and glean knowledge of the threat landscape before an event materializes.

Paste site dumps

Although an organization's sensitive information is often included in breached database dumps, this information is also often publicly exposed on paste websites like Pastebin. Over the last year, we identified over 15,000 cases of sensitive information and content (representing 18% share of total information exploitation-related events), and removed the sensitive content with 99% efficacy.

Impact of system and information exploitation

FinServ organizations and the customers they serve are increasingly at risk for system compromise. Cybercriminals have a treasure trove of valuable data at their fingertips when they gain access to a financial services organization. With this access, criminals are able to siphon customer information for resale in black markets or use it to further scam those customers directly, multiplying the return on their efforts. All the while, this tarnishes the reputation of the exploited organization and drives up remediation costs. Banks, because they are in the business of trust, cannot easily dismiss security breaches with simple apologies and promises of credit protection. Financial institutions almost always fully bare the costs of liability, account replenishment, and goodwill reestablishment - which often far exceed the actual dollar value from account losses due to the scam itself. Industry estimates place this cost at $3.92M per breach in 2019.\(^2\) Data breach regulatory fines have increased recently, with many regulatory bodies such as the Federal Trade Commission (US), Financial Conduct Authority and Prudential Regulation Authority (UK) issuing multi-million dollar penalties. Compliance regulations such as GDPR or PCI-DSS add to the costs for certain disclosure violations. For the protection of their customers, responsible FinServ organizations are obligated as well as regulated to take strong preventative measures and rapid remediation action when it comes to system compromise or data disclosure regardless of source.
Brand abuse and manipulation

Attackers take advantage of the awareness and reputation that a brand represents to its customers and the general public. Conversations, posts, and even hashtags are frequently hijacked and manipulated to influence customer interactions with the targeted brand. Logos are usurped, and sites are spoofed and made to look like carbon copies of the original. This kind of mimicry exploits the investment a FinServ organization has made in its brand, to take advantage of customers and generate profit for the attacker. Attackers seek to take advantage of the credibility of a financial institution in order to conduct further activity such as phishing, harvesting user credentials, defrauding, and otherwise taking advantage of vulnerable customers. This, in part, is due to the simplistic nature and low cost of impersonation-based attacks. Threat actors impersonate organizations and their brands in a variety of ways, but attacks against an institution’s domains and social media accounts are some of the most common. These occur across a vast and diverse array of social platforms - challenging FinServ organizations who struggle to gain visibility and timely awareness into new impersonations. ZeroFOX uses a variety of matching techniques to identify variations of account names that may include a homoglyph, whitespace characters, or other creative attempts at obfuscation by attackers. Other variants, which ZeroFOX detects and attackers utilize to increase confidence in their impersonating account, include copying the biography or image of an official account. Often these brand abuses go undetected until damage (a successful scam, for instance) has happened.

Impersonating accounts on social media

Attackers attempt to impersonate company pages, brands, or executives on social media. Imposters will use names, borrow keywords, lift trademarks and steal images from the legitimate account in order to appear more authentic prior to leveraging fake accounts for phishing or other attacks. A phishing link sent from what appears to be the social media profile of a bank will likely have a much higher click rate than a link sent by an obvious spam account. This type of impersonation is simple to do and can easily be executed against a wide range of end-users in the hopes that users will not notice they are interacting with an illegitimate account. Just as attackers impersonate corporate social accounts, they often masquerade as recognizable public figures, such as CEOs, presidents, and board members, associated with a financial institution. Impersonating an executive from a leading financial institution enables the attacker to attract and easily influence the institution’s employees and customer community - into untoward activities not to their benefit.

Spoofed and impersonating domains

Attackers often buy domains with the goal of impersonating the financial institution on social media. This may involve swapping in similar characters or appending keywords such as “help,” “support,” or other plausible concatenations to the end of the URL. Another approach used by attackers is to pick TLD country or other extensions that the legitimate domain isn’t using such as .au, .ca, .jp, .net, .biz, .gov, etc. These types of attacks trick the user into believing they are engaging with the financial organization, enabling attackers to easily conduct phishing attacks and steal a user’s legitimate credentials and other financial information that can be used or monetized.

Homoglyph attacks

In Homoglyph attacks, the basic principles of domain spoofing remain the same, but an attacker may substitute a look-a-like character of an alphabet other than the Latin alphabet. For example, the Cyrillic “а” for the Latin “a.” Although these letters are visually identical, their Unicode values differ, so that they will be processed differently by the browser. Given that there are over 100,000 existing Unicode characters, attackers have an enormous opportunity for these attacks. Impersonators also abuse homoglyph attacks to fool traditional string matching and anti-abuse algorithms.

Typosquatting

Typosquatting is another popular attack vector. If an organization has not registered domains that are close to their legitimate domain name, attackers will often purchase them to take advantage of typos. Attackers may also infringe upon trademarks by using legitimate graphics or other intellectual property to make malicious websites appear more legitimate.
Brand abuse and manipulation research findings

Brand abuse represented the greatest number of security events out of the four attack tactic categories investigated.

ZeroFOX identified over 250,000 instances where an attacker was specifically targeting a brand to abuse or manipulate. This is typically done in the form of impersonation. Brand impersonations are a foundational tactic for threat actors attempting to gain access to an organization and its customers in order to conduct large-scale attacks.

Targets of brand abuse across social media

In the last year, we identified over 530 attacks per domain, 260 attacks per brand, and 110 attacks per executive. 45% of this brand abuse occurs on Twitter. Twitter is especially attractive to actors because of the open nature of the platform - by default, Twitter user profiles are public. This makes it easy to access personal information that can be used by an actor to make an impersonating account seem more legitimate.

Significant abuse occurs on Twitter (45%), Facebook (21%), LinkedIn (11%), YouTube (10%), and Instagram (6%).

Impersonating mobile applications

A novel method of brand abuse involves the use of mobile applications that spoof those of an existing organization, or attempt to masquerade as a legitimate game or utility in order to get potential victims to download what is actually malware. Actors may look to build applications that appear to be legitimate everyday utility applications, while actually harvesting credentials, compromising the victim’s phone with additional malware, or installing adware.

Impact of brand abuse and manipulation

While it can take decades to build a strong brand, a single bad experience, such as being the victim of a scam or the breach of customer data, can materially harm brand reputation overnight with lasting effect. Although this is one of the most important attack surfaces to monitor, it is also one of the most difficult. Attacks of this nature often go undetected by organizations that are not actively taking measures to prevent them. Organizations often have a widespread digital presence, and monitoring each aspect is difficult at best. Attackers take advantage by finding an exposed surface - often a social account of a FinServ executive

- that then they can manipulate, impersonate, or even take over. This ‘soft’ vulnerability in turn allows the attacker to ultimately gain access to the executive’s followers - which they may spear phish impersonating the executive until they find a cooperating, unaware victim (another employee) that provides greater access to the financial institutions network by revealing passwords or other important data. Once the institutions network is infiltrated, the attacker has access to credentials, PII, or customer accounts, and will likely initiate stealthy extraction of this valuable data. Often the breach is discovered until months after the data is in attacker hands, customer accounts have been depleted or other monetization has begun (leading to commensurate damages).

Brand abuse and manipulation come at a high cost to FinServ organizations. In 2018, every dollar of fraud cost financial institutions $2.92, a 9% increase over costs in 2017. Not only is there the abject cost of reimbursement of stolen funds, but there is also the cost of lost consumer trust and loyalty. Brand establishment can be the single biggest investment a company makes. Negative experiences with a brand as a result of repeated abuses may cause consumers to lose faith in the brand itself and bring the brand's integrity into question — negatively impacting the bottom line or company valuation. Despite the challenges of doing so, the responsibility of proactively maintaining brand reputation and remediating abuse attempts falls squarely upon financial service organizations.
Account takeover

Account Takeover is a specific form of brand manipulation or executive impersonation where the actual owned corporate or executive social account is taken over by attackers. Social media account takeovers, in particular, threaten both brand reputation and customer trust. Not to be confused with financial account takeover, social media account takeover in this context refers to the hijacking of a social media account belonging to a FinServ's organization or executive. Once the account is in the attacker's control, the attacker has a host of exploitation options to choose from that can inflict major damage, including committing digital vandalism by changing settings or profile information in a way that tarnishes the host account's reputation, publicly posting controversial or provocative content, or messaging followers with malicious content that can be used to harvest account details, credit cards, or PII. These attacks can yield high returns for cybercriminals without the time investment of having to manage malware, command and control infrastructure and other operational security measures, often with outsized impact on the institution and its followers. While less common than other attack forms, account takeovers can have severe repercussions with lasting impact to financial institutions and their customers.

Credential compromise is a pervasive problem for financial institutions as well, particularly targeting executives and high-profile employees. These credentials often allow access to valuable information such as financial records, credit card and account numbers, and PII which is then sold by the hacker on dark web forums.

Using stolen credentials in order to log into a company's account, the attacker may then use this account to promote malicious, attacker-controlled websites that scam users or deface the financial institution's name (in the case of financial 'hacktivism'). Just as with account impersonations, account takeovers allow attackers to gain access to your customer community and leverage their trust in your brand to exploit them. Hijackers can change the account name, password, and associated email address to lock out the legitimate account owner and begin engaging with institutional followers. No accounts, whether on social media or otherwise, are completely immune to account takeover.

Account takeover research findings

While account takeovers represent only 3.55% of total security events targeting FinServ, they are often used as a springboard for more severe attacks. These attacks target both the financial institution's brand as well as its' executives in order to reach a wider customer target audience.

| FinServ executive accounts are most commonly targeted, representing 44.8% of all account takeover events, followed by FinServ brands representing 39.5% of account takeover events. |

Targets of takeover attacks

When broken down by attack target, we identified nearly 30 corporate account takeover incidents per year per institution and four account takeover attempts per executive per year.

| Nearly 40% of executives were the target or victim of an impersonation, credential compromise, or other threat. |

45% of account takeover security events discovered were related to takeover attempts on social media platforms. This includes Twitter, Instagram, Facebook, as well as LinkedIn and other social platforms.

Credential compromise

Compromised email addresses, usernames and passwords, and other account information accounted for 54% of account takeover security events in the last year. These events include any instance where an executive from a financial institution's email was found inside a breach database by the ZeroFOX Platform. Compromised credentials may provide access to a myriad of account types, but where executives are concerned, often lead to impersonation or takeover. With 23 compromised executive credentials found per day on average, this amounts to 2.3 events per executive per year analyzed as part of this report. This does not include non-executive (all other employees) credential compromises that are commonly found in breach databases.

Account role and risky settings changes

The first sign of account takeover is often a change to account settings, such as name, image, permissions, or authorized administrators. ZeroFOX identified 2,391 instances of risky role or settings changes, comprising 15.3% of total account takeover security events. These events include any unauthorized changes made to a corporate or personally owned social media account, such as name or profile picture change, or the addition of an account, administrator or permission without the explicit approval of the organization or executive.
Risky and unapproved posting on social media pages

Customers rely on financial institutions' social media accounts for important information such as office closures, account updates, and promotions. Any unauthorized posting by a bad actor on a financial organization account, particularly one containing malicious content, could put customers at risk. Also, the institution itself may be at risk - incendiary or slanderous commentary, inaccurate or misleading news stories, inappropriate disclosures, or other nefarious content could trigger marketplace reverberations that damage (or artificially inflate) stock prices, leading to class-action lawsuits and loss of trust in the institution. ZeroFOX identified 4,482 posts on financial customer-controlled social media accounts as a result of account takeover. Each of these posts either contained sensitive information (such as PII) or were posted through an unapproved (non-whitelisted) application in violation of company policy. In the most egregious cases such as hate speech or malware distribution, 213 of these posts were hidden or deleted by ZeroFOX after the associated account was locked due to suspicious activity.

Malicious direct messages sent on behalf of the organization or executive

After a successful takeover, attackers rely on public posts and direct messages to reach employees, customers, and followers. ZeroFOX identified 35 instances of malicious direct messages sent through compromised FinServ social media accounts post takeover. While this is a small portion of total account takeover security events, the implications are significant. A direct message from an official account is likely to be taken seriously, and recipients of these messages are very likely to follow an attacker’s instructions. These next-generation spear phishing techniques could be used to extort banking or credit card information from victims or to gain important and sensitive organizational information from employees.

Impact of account takeover

A takeover leading to a major breach, can cost FinServ organizations hundreds of millions of dollars or more in lost account funds, remediation costs, and regulatory penalties - not to mention loss of customer trust and stock devaluation in the marketplace. While account takeover attempts represent less than 5% of total security events targeting FinServ, they are often used as a springboard for more severe attacks. These actions target both the financial institution’s brand as well as executives in order to reach a wider audience. The business impact of an executive social media account takeover can be substantial. With the prolific use of social media, an executive serves as not only an ambassador of the organization they lead but as a representation of the organization as a whole. This is proven by the fact that global executives estimate that 44% of an organization’s market value is placed on the CEO’s reputation alone. Knowing this, protecting executives’ social media accounts from hijacking should be a top priority for FinServ, as these accounts serve as a frontline engagement tool for connecting with customers, prospects, and employees. It is therefore imperative that a financial institution ensures the only accounts interacting with their clientele are their own, and not at the risk of damaging reputation and customer trust.

Fraud and scams

Social networks are frequently used by financial institutions for marketing, advertising, and customer service. They have even become points of sale themselves. Unsurprisingly, scammers have also flocked to social platforms to extort businesses, their employees, and their customers. Social media scams often involve social engineering victims into directly sending money. Scammers initially lure their victims into engaging through public posts. Broadcasting mechanisms like hashtags and mentions are used to maximize audience size and relevancy before the most responsive users are targeted individually. Potential victims are encouraged to follow up privately through direct message (DM), phone call, text message, or on other social networks. If a scammer can convince a potential victim to continue a conversation outside of the original platform of contact, especially via email, text, or phone call, the interaction can better be personalized, and the scammer avoids potential scrutiny from the original social network.

Common social media scams

Scammers promote a variety of ‘money flipping’ and other financial scams on social media. One of the most popular of these involves scammers alleging that they can transfer “unclaimed funds” if a banking customer hands over their login information. Similarly, card-cracking scams involve convincing banking customers to provide a scammer with credit card and banking details. The scammer then deposits funds into the account using fraudulent checks and immediately withdraws the funds from an ATM. People tend to fall for these types of scams because they are promised a cut of the funds, and that there will be no legal repercussions for their role in the scam since they are solely a temporary ‘middleman’ in the transaction.
Fraud and scams research findings

During the 12 month period, ZeroFOX identified just under 88,000 indications of scams and financial fraud, across 25 data sources. 37% of these security events were identified as money flipping scams, with another 28% classified as customer giveaways and coupon scams. Scams of this nature promise that an item, some kind of service or money, will be given away or that the victim will receive a valuable coupon if they provide personal or financial information to the scammer.

Where fraud and scams occur

Financial frauds and scams are most commonly seen on Twitter (40%), Instagram (31%), and the dark web (15%).

Public social media platforms allow scammers to cast a wide net for their potential victims, and public Twitter and Instagram accounts are relatively commonplace. Financial fraud is rampant on the dark web, where credit card information and banking credentials are sold en-masse for affordable prices. According to Experian, a global credit-reporting agency, individual credit card info is sold on the dark web for as low as $5 to over $100. ZeroFOX identified 55,312 posts on dark web or paste sites advertising the sale of stolen credit card information just in the last year. This financial information is obtained by criminals in many different ways, but phishing and banking trojans — a type of malware specifically focused on stealing banking and credit card information — are some of the most common methods. Banking trojans, apps that disguise themselves as genuine apps so as to access your banking details, are persistently a concern for bank fraud given their scale, efficacy, and ability to be quickly modified and updated. Increasingly, they target high profile individuals for their corporate access, with potentially larger account balances to siphon, and not simply for individual data.

Cryptoscams

Cryptoscams also encompass a large percentage of this data set - over 23,000 cryptoscam events were identified, with 27% of them including a wallet ID within the post itself. Some of the more common cryptoscams involve fake cryptocurrency exchanges that promise to send a victim money if they send bitcoin to a fraudulent wallet ID. Additional scams involve crypto Ponzi schemes, fake initial currency offerings, and fraudulent wallets. Many of these scams abuse Open Graph Protocol, which is responsible for the website previews of links included in social media posts. This can be used to make a malicious link much less obvious - as the website preview will be seen rather than the malicious link.

Impact of financial fraud and scams

Most scams sound too good to be true. Even so, people do fall for them, perhaps out of desperation or hope that the scam may be legitimate. Ultimately, financial institutions are the ones who absorb the cost of fraud. In addition to the actual financial cost of stolen account funds, there is the added real cost related to retrieval efforts, credit remediation and protection costs. Compounding this are the intangible costs due to harmed brand reputation and lost consumer trust for the financial institution in question. Unfortunately, these intangibles can dwarf the tangible costs of funds loss. Anti-money laundering and breach protection laws may place additional penalties on violators, especially for organizations not exhibiting adequate controls. For these reasons, overseeing and constant monitoring for brand impersonations, attacker forum discussion and dark web activity are the best methods to obtain early warning and detect and prevent fraud for financial institutions. At the very least, you can better prepare for future attacks if you gain awareness during attack planning stages.

Case Study

Check Forging Scam

When famous or influential people promote these types of scams, as in the recent case of the Bronx-based rapper known as Young Ash, they tend to be particularly successful. Using social media platforms like Snapchat and Instagram, the rapper made over $50,000 by forging checks using financial information obtained from victims who fell for the scam. These checks were deposited into victim’s accounts before the amount was withdrawn by either Ashley or one of her accomplices. Allegedly, the group deposited over 52 counterfeit checks.
Conclusion & Recommendations

Digital platforms continue to be a valuable resource for both financial services organizations — and cybercriminals, too. Increasingly, cybercriminals are operating outside the bounds of traditional security perimeters. In just 15 minutes, someone can access forums, sellers and fencers of credit card data and other PII, as ZeroFOX Alpha Team has shown. Fraudsters operate in their own ecosystem via forums and the dark web, but are not afraid to spread their reach onto platforms that the everyday user logs onto.

Despite the risks of being present on these platforms, the digital world provides FinServ organizations the opportunity to better connect with consumers, engage customers, and to extend and control their marketing and messaging. By monitoring their digital presence and mitigating the risk associated with it, financial institutions are able to optimize their utilization of the digital space and do so safely.

Regardless of the source or reason for a disclosure, FinServ customers expect their financial services institution will take every precaution and make every remediation effort necessary to protect their account and personal information from misuse. They are entrusting these organizations with some of their most valuable assets: their identities, money, and investments.

Organizations who wish to mitigate their risk on social and digital channels can take a number of steps. ZeroFOX recommends the following:

**Institutional recommendations**

- Monitor and protect all digital and social media platforms. You cannot mitigate a threat unless you are aware of its existence.
- Apply risk-appropriate protection and privacy policies across the organization.
- Complement human research with intelligent machine-based analysis to automate the collection and processing of indicators and alerts.
- Educate your employees to encourage compliance with policies and standards pertaining to social media, phishing attacks, and other risks specific to your company.
- Correlating additional indicators helps validate and eliminate false positives, which allows for rapid remediation and minimization of brand abuse.
- Integrate filtered or curated threat intelligence specific to your threat environment to better prioritize and surface relevant alerts.
- Credentials and information are often hiding in plain sight. Monitoring paste sites and social platforms can help to mitigate information leakage.

**Individual recommendations**

- Enable 2-factor authentication on all of your social accounts and assets. Multi-factor authentication helps reduce your risk of account takeover.
- Ensure privacy settings are up-to-date. Social and digital platforms are known to change these occasionally as they roll out updates and other improvements. If you are unsure of what each field translates to in the corresponding UI, log out and search for yourself on the social or digital network to see what information is publicly available.
- Within the ZeroFOX security platform, customers can use the social search bars to ensure their digital identity has not been compromised by impersonation accounts. The ZeroFOX platform is also able to automate this process.
Methodology

Over the course of this comprehensive one-year study the ZeroFOX Alpha Team, ZeroFOX’s threat research organization, leveraging the ZeroFOX Platform, collectively analyzed over 2.9 billion pieces of content. The data discussed in this report was collected over a twelve-month time period from May 1, 2018 - May 1, 2019, inclusive of a wide variety of sources consumed by ZeroFOX. This includes data from thousands of discrete data sources, including all major social media networks such as Facebook, Twitter, Instagram, and other regional networks. It also includes covert communication channels like Telegram and IRC, dark web data sources and attacker discussion forums, paste and code sharing sites like Pastebin, Bitbucket, Github, and more.

The findings in this report are based on comprehensive threat data collected across ZeroFOX’s ecosystem of financial services customers, including banks, brokerages, cryptocurrency exchanges, credit unions, credit reporting agencies, insurance providers, and investment firms. ZeroFOX has a very strong presence in the financial services industry, with thousands of FinServ users, spanning over 50 countries and geographical regions. Based on our experiences within this sector, we believe this provides a fair and accurate representation of the Financial Services industry overall.

The ZeroFOX Platform analyzes this wide array of data in near real-time, and employs a combination of methods to determine when threat activity or content is seen that may be indicative of a pending or in-progress attack. Suspicious content or activity generates an alert, or a security event, on the ZeroFOX Platform. These alerts are reviewed and validated by our global security operations team. If an alert is deemed to be critical and/or the offending item violates the terms of service of a network platform, the ZeroFOX team may request a takedown of the content or account in question. A takedown as related to remediation is the removal of an impersonation account, a spoofed domain, or a piece of content that otherwise violates network Terms of Service (ToS).

Of the 2.9 billion pieces of content analyzed within this timeframe, ZeroFOX detected over 8.9 million security events and conducted over 98,000 takedowns.
Sources

About ZeroFOX

ZeroFOX, the innovator of digital visibility and protection, protects modern organizations from the dynamic risks of social media and digital channels. Each day, ZeroFOX’s cloud-based SaaS platform processes millions of posts and accounts across the social landscape, spanning Facebook, LinkedIn, Twitter, Instagram, YouTube, and more. Using targeted data collection, intelligent analysis, and automated remediation, ZeroFOX protects businesses and government agencies around the world against phishing attacks, information loss, account compromise, fraud, compliance violations, and financial loss. Led by a team of information security and high-growth company veterans, ZeroFOX has raised nearly $100M in funding from NEA, Highland Capital, Silver Lake Waterman, Redline Capital and others, and has collected top industry awards such as Red Herring North America Top 100, the SINET16 Champion, Dark Reading’s Top Security Startups to Watch, Tech Council of Maryland’s Technology Company of the Year and the Security Tech Trailblazer of the Year.

In order to battle the rapidly changing cybercriminal underground, ZeroFOX works diligently with our financial customers to provide discovery, coverage, monitoring and comprehensive remediation across all levels of financial cybercrime. One of the best parts of this practice, sharpened over the years, is that the ZeroFOX ecosystem is the biggest weapon that defenders have against would-be attackers. As we have grown, so has our visibility and ability to make connections across data points.

ZeroFOX Alpha Team

ZeroFOX Alpha Team is a unique threat research organization within ZeroFOX dedicated to investigating malicious activity on social media and digital platforms to better understand how to protect people and organizations alike. Our group is composed of curious and determined scientists, engineers, and writers; techies and storytellers. We are committed to integrity in all aspects of our research process, from data collection to reporting. No confidential customer information is contained in the report.