# Responding to COVID-19

**Focus on combating cyber fraud in the Financial Services Industry**

The global spread of COVID-19 has led to an abrupt shift in the everyday lives of the world’s population, temporary closures of cities and businesses, and widespread panic. Attacker have taken advantage of this unprecedented situation, targeting vulnerable and unsuspecting individuals, companies, and government agencies. While financial services organizations have been long focused on cyber risks as compared to other industries; a surge in opportunistic bad actors due to COVID-19 requires continued vigilance – 41% of responding organizations believe a security breach contributes to major operational disruption and loss of customer trust. As financial services organizations adapt to the new normal (e.g., remote operations, surges in transaction volumes, sustained dependencies on third parties) and participate in/administer stimulus funds and other benefits; there are a number of steps that can be taken to help reduce the risk of cyber fraud.

## COVID-19 cyber risk and fraud use cases

<table>
<thead>
<tr>
<th>Remote financial services operations</th>
<th>Transaction volumes</th>
<th>Benefits administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Context: Shelter-in-place and mandatory work from home guidance has resulted in large-scale remote working arrangements and greater remote delivery of financial services. Without sufficient identity verification and interaction lifecycle monitoring, malicious actors can use stolen financial information to make fraudulent transactions.</td>
<td>- Context: A large increase in network and transaction traffic volume (e.g., order, trades/trade management, operations) can place IT infrastructure and business applications under severe stress resulting in increased number of margin calls, delayed orders, bypassed risk/fraud/money laundering controls. This can lead to account takeovers, unauthorized transactions, etc.</td>
<td>- Context: Banks are currently supporting administration of loans from the CARES (Coronavirus Aid, Relief, and Economic Security Act) Act. Insurance providers will also be faced with a rise in the number of asset/health insurance claims. Malicious actors may phish/social engineer personal information from individuals and raise fake benefit claims.</td>
</tr>
</tbody>
</table>

## Insider threat

- Context: Employees/third parties with access to sensitive systems (e.g., transaction systems, trading platforms) are working remotely. Extensive virtual workplaces impact morale and can heighten risk of insider activity. Some systems (e.g., trading systems) were not designed to securely facilitate remote working and can lead to breakdown in controls including risky leverages and insecure communications and trading activity.

## Third parties

- Context: Third-party service providers who perform critical functions need to secure delivery of such services while dealing with a spike in traffic. Service providers who are not able to deal with such a surge in transactions or do not have appropriate security controls may be more easily compromised by adversaries.

## Top cyber threats

### Malware & ransomware

Malware lends its name to variants of malicious software—including viruses, ransomware, spyware, etc.—intended to cause harm to a user, system, or organization. Ransomware is an increasingly popular malware that restricts or limits users and organizations from accessing their systems and data until a ransom or release fee is paid. For example: user downloads COVID-related mobile app, which instead encrypts their device until a sum is paid.

### Insider threat

When organizations have employees, contractors/business associates—who have information regarding the organization’s security practices, data, and computer systems—working remotely for an extended period of time, there is an increased risk of malicious insider activity. For example: due to a downturn in the market, an employee may lose their job and this can lead an individual to retaliate against the company either by stealing information, causing system disruptions etc.

### Threat actors employ COVID-19-themed social engineering and phishing techniques to steal sensitive information such as usernames, passwords, or credit card details for nefarious purposes like identity and financial fraud. According to our research, phishing is ranked with malware as a top cyber threat organizations face amongst organizations surveyed.

For example: attacker sends an email posing as government agency asking for sensitive personal information and bank account details in order for the individual to obtain their CARES Act loan. With such details in hand, the attacker can raise a fraudulent CARES Act loan request.

### Vulnerable platforms

Organizations cannot let these uncertain and unprecedented times distract them from the assumption that sensitive data is constantly at risk for attack. Many organizations will need to maintain their current data protection activities, while some organizations handling extra data volume should opt for increased protection measures (e.g., loan processing platforms, transaction platforms).

For example: a company’s endpoint security controls are not effective for a small business loan processing platform, resulting in an adversary being able to exfiltrate sensitive data.

---

1. Deloitte Future of Cyber Survey 2019
2. Deloitte - FS-OAC Benchmarking survey 2018
Respond now

**Verify identity**
✓ Implement strong identity proofing measures to establish new user and customer accounts
✓ Create or enable secure login features, including complex password requirements, multi-factor authentication (MFA), one-time passwords, biometrics or knowledge-based authentication (KBA), or leverage existing authentication capabilities such as those for know your customer (KYC) initiatives
✓ Review and determine access to the network is controlled through VPN use, as well as increased monitoring or personnel with elevated system permissions and privileged access

**Implement proper “plumbing”**
✓ Secure collaboration software and provide work from home guidance
✓ Regularly patch data protection software (e.g., antivirus or antimalware)
✓ Review and update data protection policies and controls, including scaling data protection services to match increased volume when facing network capacity issues
✓ Utilize DIME (data-in-motion encryption) and DARE (data-at-rest encryption) to safeguard sensitive data
✓ Confirm patching for critical IT systems, mobile assets, and devices including bring your own device (BYOD)
✓ Bolster security guardrails for cloud environments and hosted applications

**Adjust baseline of monitoring and behavior patterns**
✓ Drive closer engagement between security and fraud teams for faster detection of fraudulent activity
✓ Leverage customer profiling and time-on-file techniques to maintain the customer experience and confirm service availability to perform valid transactions
✓ Enhance monitoring rules and configurations to account for new traffic patterns, remote working use cases, etc.
✓ Enhance session monitoring controls for sensitive and privileged access
✓ Enable enhanced monitoring of third-party activity and continuously evaluate readiness to deal with COVID-19-related threats

**Proactive stakeholder communication**
✓ Promote extended enterprise awareness of threats, specifically social engineering activities which may be particularly effective in the current environment
✓ Communicate ways to pinpoint threats from electronic communications (e.g., unsecured webpages, mimicked email addresses, grammatical errors, and crude website design)
✓ Instruct employees on protection measures for personally identifiable information (PII) or financial information
✓ Engage regulators proactively and provide periodic updates on COVID-19-related preparedness measures

**Takeaways**
During this chaotic time, it is critically important that organizations **build trust with customers** as they continue to deliver—and adapt—their mission in the face of pandemic-driven disruption. Under normal business operations, organizations cite embedding security into products and services as a top priority; even in the face of uncertainty, **security should be prioritized in back and front office operations**.

Financial institutions should continue to proactively monitor for fraudulent cyber schemes and **share insights broadly as fighting cyber crime is a collective effort**.

**Bolstering basic cyber hygiene** along with **enhancing capabilities** for the next normal can enhance customer trust and security, setting the stage for business viability post-pandemic.

1. Driving closer integration between security and fraud teams through the enterprise anti-fraud framework
2. Communicating with stakeholders to manage expectations and build trust
3. Scaling security controls for long-term persistent strain on technology resources
4. Enhancing monitoring of insider and third-party activity
5. Adapting employee trainings and policies based on lessons learned

**Contact:** Coronavirus Response | USCyberCoronavirusResponse@deloitte.com

Deborah Golden
Principal
Deloitte & Touche LLP
debgolden@deloitte.com

Adam Thomas
Principal
Deloitte & Touche LLP
adathomas@deloitte.com

Sameer Airyil
Senior Manager
Deloitte & Touche LLP
sairyil@deloitte.com

Mark Nicholson
Principal
Deloitte & Touche LLP
manicholson@deloitte.com

Daniel Soo
Principal
Deloitte & Touche LLP
dsoo@deloitte.com

Copyright © 2020 Deloitte Development LLC. All rights reserved.

*This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.*

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.