# Cybersecurity for FMIs

FINANCIAL INCLUSION GLOBAL INITIATIVE

NOVEMBER 2020

## Fourth edition of the FIGI Cybersecurity for Financial Market Infrastructures Newsletter

The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructure (CPMI), and the International Telecommunications Union (ITU) funded by the **Bill & Melinda Gates Foundation** (BMGF) to support and accelerate the implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global **'Universal Financial Access 2020'** goal. FIGI funds national implementations in three countries—China, Egypt and Mexico; supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) electronic payment acceptance, (2) digital ID for financial services, and (3) security; and hosts three annual symposia to gather national authorities, the private sector, and the engaged public on relevant topics and to share emerging insights from the working groups and country programs.

The FIGI Cybersecurity for Financial Market Infrastructure Workstream, led by the WBG as part of the Security, Infrastructure and Trust (SIT) Working Group, aims to explore compliance and best practices for cybersecurity specifically on financial infrastructures. The Workstream aims to develop a toolkit of resources and materials for awareness and education for policymakers and related and plans to further develop methodologies, standards and good practices on cybersecurity for financial market infrastructures over the course of the FIGI project.

This newsletter aims to update you on the latest developments in cybersecurity, cyber events and security breaches. We hope you find this newsletter useful and welcome your feedback.

Sincerely,
**FIGI Secretariat**

*Managed by*

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

## Inside this Edition



## A Regulator's Perspective

**COVID-19 related fraud and money laundering trends**

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) prepared a special bulletin on the trends of money laundering and fraud during Covid-19. The bulletin focuses on areas that may pose an increased money laundering risk and is based on an analysis of COVID-19-related transaction reporting and fraud reporting. Highlights include the identification of unusual transaction activities and an explanation of how to identify between financial activity related to the pandemic versus attempts to profit from the current situation to undertake or facilitate money laundering. Common Covid-19 fraud trends include an increase in specific categories of fraud related to an increased reliance on virtual currencies and traditional payment methods offered by financial institutions (i.e., credit card payments, eTransfers and wire transfers). Reports related to phishing schemes, identity fraud and merchandise scams have accounted for 80% of the COVID-19 related fraud, and the CAFC expects that it is likely to see in an increase in loan scams, debt consolidation frauds, and investment

*continued on page 2*

***A Regulator's Perspective,*** *continued from page 2*

fraud as well as cyber dependent frauds such as spear phishing, ransomware and phishing campaigns. (**Read the full article here**)

- **New financial protection watchdog agency proposed in California**
  Lawmakers in California are moving quickly to create a new department under the state government to enforce financial consumer protections, according to NPR. While the Consumer Financial Protection Bureau (CFPB) is typically responsible for consumer protection in the financial sector, NPR reports enforcement is currently down 80 percent from 2015, and money returned to consumers has dropped by 96 percent. Since the outbreak, complaints about financial wrongdoing have increased by 40 percent in California, including disputes about mortgages, personal loans and firms that promise to get consumers out of debt. Small business groups and financial firms are largely in favor of the measure. (**Read the full article here**)

- **Industry associations formed to tackle Cybercrime**
  **The Wall Street Journal** reported a 35 percent jump in year-over-year credit card fraud in April 2020, with malicious actors harnessing phishing schemes and brute-force hacking attacks to swindle data and funds. Mobile banking apps have also been frequently targeted, and breaches are expected to be on the rise in the coming months, according to the FBI. The agency recently warned against a variety of different **mobile banking hacking** attempts, with some hackers deploying fake apps that steal users' login information, and others leveraging trojan viruses to infiltrate user accounts. Financial institutions are addressing these issues by coordinating to form industry associations, such as the **Cyber Risk Institute** (CRI). The CRI aims to create cybersecurity standards and develop a new list of cybersecurity guidelines and best practices for Financial Institutions to follow. (**Read the full article here**)

- **Collaborative efforts to strengthen Digital Finance Cybersecurity**
  In a stakeholder **workshop** organized earlier this year by CGAP (Consultative Group to Assist the Poor) on cybersecurity in emerging financial markets, industry players considered the challenges posed by cybercrime and identified two main ways to help financial service providers become more cyber-resilient: (i) Harmonizing industry standards, which includes partnership agreements, industry associations and local regulatory requirements are seldom uniform, making compliance management a difficult task, especially across markets; and (ii) Collaborating across the ecosystem, which includes to sector players such as banks, mobile money providers and other third-party providers in the financial ecosystem coordinating to share intelligence and create solutions to address cybersecurity challenges. Harmonized standards and more collaboration would improve cybersecurity risk management practices in digital financial services. (**Read the full article here**)

## Cryptocurrency Corner

- **Crypto laundering operation disrupted in Ukraine**
  A cryptocurrency trading platform, Binance, helped to identify a cybercrime organization behind an alleged money laundering effort. The platform worked in collaboration with Ukraine's Cyber Police to identify and detain cybercriminal group behind alleged ransomware activities and laundering of over **$42 million in digital currencies** over the past two years. According to the company, continued collaboration with the authorities is a driving force in boosting secure cryptocurrency adoption and improving the image of the greater crypto space. (**Read the full article here**)

- **DOJ dismantles three terrorist financing cyber-enabled campaigns**
  The U.S. Department of Justice (DOJ) intercepted three cryptocurrency campaigns that were funding terrorist groups. According to a **press release.** U.S. authorities seized over 300 cryptocurrency accounts holding millions of dollars that the three groups amassed by donations via social media. The donations were solicited both by advertising their campaigns and by claiming that the money went to charities or to fake businesses selling N95 face masks. The DOJ also uncovered four websites and four Facebook pages related to the groups. (**Read the full article here**)

*continued on page 3*

# Cybersecurity Events and Breaches

- **Online government portals in Canada shutdown due to cyber breach**

  A cyberattack directed at two dozen Canadian government platforms led to the shutdown of most of its online portals for two days. As a result of the breach, the Canadian Revenue Authority (CRA) reported that more than 11,000 of 12 million personal accounts were compromised, including online portals related to taxpayer data and COVID-19 relief programs. Canada's Centre for Cyber Security (the agency that leads the government's response to cybersecurity attacks) found that the credentials used in the attack came from previous unrelated data breaches, where account owners reused old passwords on Government of Canada systems. (**Read the full article here**)

- **DOJ shuts down fraudulent websites over pandemic-related fraud**

  As part of its ongoing efforts to stop coronavirus-related fraud, the U.S. Department of Justice (DOJ) obtained a temporary restraining order to combat fraud related to the coronavirus pandemic that targeted vulnerable populations through financial fraud schemes, the importation of counterfeit pharmaceuticals and medical supplies, and illicit websites defrauding consumers which compromise legitimate trade and financial systems. The DOJ recommends a number of precautionary measures, a few of which including the following: Independently verify the identity of any company, charity, or individual that reaches out regarding COVID-19; be wary of unsolicited emails; check online reviews of any company offering COVID-19 products or supplies; and be cautious of "investment opportunities" tied to COVID-19. (**Read the full article here**)

- **Malware found embedded in Chinese Tax Invoicing Software**

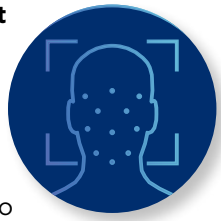
  China's process of VAT tax invoicing is centralized through the "Golden Tax Project", for which businesses are required to use one of two official providers of tax for payment of VAT taxes. Malware, called 'GoldenHelper', was found in the software for one of the providers, and the spyware contains a hidden backdoor capable of remotely executing arbitrary code with system level privileges. While the malware was quickly identified and the spyware deployment mechanism is no longer be active, it is unclear whether the overall threat presented by the spyware program has been diminished. (**Read the full article here**)

# Developments in Payments Security

- **Mastercard introduces new tokenization technology to combat fraud**

  As e-commerce increases due to the COVID-19 pandemic, Mastercard has introduced new tokenization technology, MDES for Merchants (M4M), designed to protect security of consumers and merchants as shopping goes increasingly digital. This aims to foster cybersecurity and combat fraud in Saudi Arabia and Jordan, and across the Middle East and North Africa. Tokenization encrypts consumer data by replacing card numbers with digital tokens. Every time a transaction is made online or with a mobile wallet, a unique token is created to make the payment and ensures that a consumer's 16-digit card number is not stored anywhere. This prevents improper usage at any other location and provides additional security to minimize online fraud. (**Read the full article here**)

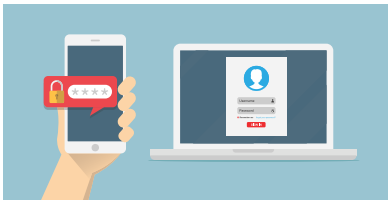
- **Facial recognition firm receives grant for biometric fraud detection**



  A fund set up to foster competition in the banking sector in the UK, **Banking Competition Remedies**, has awarded $6.6 million in funding to facial recognition firm Onfido, to invest in the development of biometric fraud detection, data anonymization, and document fraud prevention technologies. This will occur concurrently with the development of portable identity (PID), in order to integrate these technologies and provide a service which minimizes the impact of the KYB (know your business) process on SMEs. (**Read the full article here**)

- **Collaboration to develop secure text-based transactions**

  A firm specializing in digital identity verification services called **Mitek** has partnered with an identity verification and eSignatures firm, **Lightico**, to provide a new way to complete transactions over text message. The latter uses a secure platform to allow businesses to collect forms, documents, eSignatures, photos and payments, consent to disclosures, and to verify identities instantly via text. Lightico uses Mitek's Mobile Verify with Face Compare and Mobile Fill to authenticate the identity of those using its service which provides security. (**Read the full article here**)



- **Using Cloud technology to improve payments**

  A typical payment flows through about four different banks before the payment is complete, with each bank conducting its own regulatory and compliance checks. These checks are necessary to counter the other major threats facing payments. Banks and payment providers are increasingly using cloud-based payment options to mitigate these flaws. One **study** from Gartner found that off-premise cloud infrastructure experienced 60 percent fewer incidents than traditional data centers, as the former have built-in security controls, including monitoring and surveillance. For these reasons, banks are increasingly outsourcing their payments infrastructures to third-party cloud providers. (**Read the full article here**)

- **Identity Trust Platform uses AI to identify fraudsters**

  An AI-driven identity trust platform called **Kount** has developed artificial intelligence (AI) that can assess multiple data points quickly to determine if the person is who they say they are, or at least within a very high probability. This is particularly important now, where consumers and businesses alike have nearly entirely reoriented themselves around digital platforms. Where consumers go, businesses are following—including companies that have never (or barely) transacted online before, and those that have but never at the scale they are currently being called to provide. This can be a target for fraudsters, as increases in account takeovers have been observed in eCommerce, gaming and streaming. (**Read the full article here**)

- **Fighting online fraud through stronger authentication of digital transactions**

  Preparing against fraudulent actors involves being vigilant about both old and new vectors of attack. This could include social engineering, synthetic IDs, bank identification number (BIN) attacks, or the use of card generators to create many potential card numbers (which rely on probing card-authorization systems to see which ones are valid numbers), among other methods. Banks need to establish multiple layers of protection, primarily through identity verification. Mastercard has been making some efforts in this direction including: using a series of direct identity challenges and biometrics to establish that the party on the other side of the transaction is who they say they are; collaborating with consumers to monitor the activity on their cards; opt to turn their cards on an off; and offering ID Theft Protection. (**Read the full article here**)

# Opinions, Research and Publications

**Increasing cyber investment to create new European office and data center demand**

A growing number of European cyber-attacks have attracted EUR2.3 billion of venture capital investment into European headquartered cybersecurity companies during the last five years. The UK accounted for EUR1.3 billion of the five-year total, led by France (EUR316 million), Switzerland (EUR303 million), Ireland (EUR70 million), Germany (EUR68 million) and Spain (EUR36 million). With both the number of employees working from home on their personal devices and the number of cyber-attacks having increased since Covid-19, investment into cybersecurity is expected to increase even further. (**Read the full article here**)

**Regional Centers Can Help Low-Income Countries Build Cyber Resilience**

Cybersecurity resource centers can prove to be beneficial for the financial sector by facilitating the: (i) exchange of information between public and private actors about cyber threats, lessons learned, good practices and opportunities for collaboration in research and innovation on a greatly increased scale; (ii) provision of cybersecurity services at more affordable prices than what is currently available—primarily from vendors that cater to higher GDP economies—due to the sharing of capital expenses and staff salaries; (iii) provision of specialized expertise and guidance for the financial sector and for providers working with lower-income customers who may be at higher risk for cyberattacks due to their lower levels of digital literacy, cyber awareness and use of less secure transmission channels. They can also potentially facilitate international collaboration. (**Read the full article here**)

**Rethinking Cybersecurity for a post-pandemic world**

Over the previous months, the cybersecurity community has observed numerous attack vectors that use a COVID-19 theme either as bait or as a way to conceal malicious activity from easy identification and detection. The cybersecurity community has become aware of numerous attempts to mimic informational applications, and that malicious activities can occur underneath a good-looking infection map or fictitious 'infection radar'. These campaigns have been noticed at a higher frequency in regions where there has been a surge in COVID-19 infections, i.e. threat campaigns directly correlate to the number of infections and public perception of the pandemic—when people are more anxious, threat actors increase their exploitation of the COVID-19 theme.
(**Read the full article here**)

**A phased approach to mitigate risks from rapid unplanned digitization**

COVID-19 is accelerating the digital transformation of business, especially retail, education and healthcare. Rapid, unplanned digitization increases the risk and impact of cyberattacks. Leaders, tasked with securing their businesses from both market forces and cyberattacks, need to take a systemic approach to cybersecurity

**Shared Cybersecurity Resource Centers**


Shared cybersecurity resource centers may operate at the continental, regional and country levels.

*Source:* CGAP: https://www.cgap.org/blog/regional-centers-can-help-low-income-countries-build-cyber-resilience

***Opinions, Research and Publications,***
*continued from page 5*

in three phases: (i) Immediate Term (0 to 3 months): To keep enterprises running, businesses must secure remote access and collaboration services, step up anti-phishing efforts and strengthen business continuity; (ii) Near Term (3 to 6 months): Securing end users, data and brand is the next priority. As the number of cybersecurity threats have increased, CSOs and their teams will also benefit from increased prioritization; (iii) Medium to Long Term (12 months): Cybersecurity strategists also need to think longer term, about the security of their processes and architectures, including automation to improve the security of remote users, devices and data. (**Read the full article here**)

**Cybersecurity measures to prepare for the new normal post COVID-19**

Effective cyber resilience requires a combined and aligned multi-disciplinary effort to move beyond compliance to cohesive business and digital enablement. It is imperative that leaders strategically manage information risks, work towards a culture of shared cyber-risk ownership across organizations and take a strategic approach to cyber resilience. These measures include: (i) fostering a culture of cyber resilience; (ii) focusing on protecting critical capabilities and services; (iii) balancing risk-informed decisions during and after the crisis; (iv) updating and practicing response and business continuity plans as the business transitions to the new normal; and (v) strengthening ecosystem-wide collaboration, including taking a systemic approach to cyber-risk management.
(**Read the full article here**)

**FIGI Cybersecurity for FMIs Information:**
For any questions, comments or to unsubscribe from this newsletter please contact the FIGI Secretariat **(figisecretariat @worldbank.org)** and Renuka Pai (**rpai@worldbank.org).**