How digital transformation increases consumer and retail fraud risks

Digital transformation has swept across the Consumer Products & Retail (CPR) sector, from manufacturing process automation, to sales and distribution, and logistics and digitization of customer payments. Yet, as CPR companies adopt impressive new technologies, they also encounter new fraud risks.

This paper examines the emergent digital fraud dynamics when organizations undergo a digital transformation journey. The EY Forensics team outline ways that companies can address loopholes, tackle misconduct and put in place monitoring mechanisms to potentially preempt and mitigate fraud.

What is driving the digital transformation in CPR?

Direct-to-consumer brands are accelerating their digital transformation. The e-retail market has grown by more than 100% a year over the past five years and in 2017, e-retail sales accounted for 10.2% of global retail sales,[1] with the fastest growing online retail markets being Indonesia, India, Mexico and China. In 2019, e-retail sales are set to account for up to one-third of total retail sales in China.[2]

Consumer expectations are changing as direct-to-consumer brands acquire individual customers at scale, forcing traditional retailers to move online themselves. Omni-channel retail has now become the new normal. Retailers need to align their product portfolio and customer experience with consumer preferences and behaviors to increase sales and compete effectively.

The CPR industry has responded to consumer expectations — for speed, ease and convenience — by transforming the point of sale (PoS) process in traditional retail stores, online platforms for direct consumer reach, as well as the supply chain systems that expedite the ordering and purchasing process. Investing in technology, such as a distribution management system (DMS) for tracking secondary sales (distributor to retailer), PoS terminals for tertiary sales (retailer to consumer), and sales force automation software for performance monitoring and sales route optimization has helped companies on the path to digitization.

> “The e-retail market has grown by more than 100% a year over the past five years and in 2017, e-retail sales accounted for 10.2% of global retail sales, with the fastest growing online retail markets being Indonesia, India, Mexico and China.

Digitization allows suppliers and consumers to access fast-growing emerging markets and enables multidirectional supply chains connecting importers and exporters, suppliers, carriers, distributors and customers. E-commerce extends customer choice with faster service and more products via multiple channels. In addition, e-commerce offers multiple payment options and online interaction between retailers and customers, including chat features and order tracking. Retailers have a clearer audit trail, richer transaction data and a direct feedback loop along with the potential to reduce customer services staff while adding rapid response to the customer experience.

Digital transformation is reshaping CPR behind the scenes as automation streamlines manufacturing, logistics and payments, and expedites integration with third-party networks that link subcontractors, manufacturers, stockists and distributors. These processes produce real-time data, which can be used for more precise management and monitoring. This includes monitoring of trade and distribution spends, brand visibility promotions, as well as tracking secondary sales at distributor and retailer level. On the customer side, data is leveraged to reduce order processing and delivery times, as well as to enable targeted and personalized sales, which fuels marketing and product development in line with consumer trends and preferences.

[1] “Annual retail e-commerce sales growth worldwide from 2014 to 2021,” *Statista*, statista.com/statistics/288487/forecast-of-global-b2c-e-commerce-growth/, accessed 11 March 2019.

[2] “E-commerce share of total global retail sales from 2015 to 2021,” *Statista*, statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/, accessed 11 March 2019.

Emergent problems

As more stakeholders — vendors, suppliers, distributors, retailers and sales teams — use digitized technology, such as automated operational processes, real-time data analysis and digital payments, the risk landscape is changing too. Incidents of fraud perpetrated by company insiders, connected organizations and external parties are exposing and exploiting the new vulnerabilities of networked business models.

Digitization has focused concerns on fraud. The EY *15th Global Fraud Survey*[3] found that 36% of respondents considered fraud and corruption as the greatest risk to business and 37% rated cyber attack as the greatest risk.

The primary vulnerabilities faced by the CPR sector are:

- **Sensitive personal data collected through e-commerce:** Retailers are targeted because they hold up-to-date data that criminals can use, such as names, addresses and credit card details. High-profile hacks have business and reputational consequences for companies
- **Cyber threats to online transaction platform:** Denial-of-service or distributed denial-of-service (DoS or DDoS) attacks represent a major business risk as sales are halted whenever the website is down. This can be the result of a malicious attack or a system failure because the platform has not been configured to respond to the volume of traffic on peak sales days, such as Black Friday
- **Insider risk:** Fraud involving company employees misusing internal systems and processes (see *Incidents of fraud in sales systems* p6)

Proactive fraud risk assessments have uncovered specific examples of the above-mentioned vulnerabilities affecting CPR companies, such as scams involving loyalty card sharing, bulk buying to collect loyalty points and resale of goods in the gray market.

Digitization links online systems and physical processes, sharing real-time data between internal functions and third parties to reduce order response times and mitigate overstocked inventories. This opens up new vulnerabilities, particularly when companies fail to upgrade control and monitoring measures. These include:

PoS: Digitization has transformed the PoS functionality by recording and aggregating transactional data. However, PoS is also a major target for fraud, opening up in-store retail to e-commerce vulnerabilities. Some of the common vulnerabilities include:

- The risk of the terminal itself being targeted — mobile PoS devices being vulnerable to malware via in-store Wi-Fi networks
- Most terminals accepting contactless payments, including via apps, which present additional risks around authentication and security for rapid customer onboarding
- Self-service checkouts that attract fraud perpetrated by customers, for example scanning one item and packing another more expensive item, or several items

In emerging markets, modern trade businesses face issues like wholesale outlets purchasing high-discount necessity consumer goods in high volumes from the store — resulting in stock-outs (products becoming out of stock) and thereby, drop in footfall and a reduction in repeated visits from the customer.

[3] "Integrity in the spotlight: The future of compliance," *15th Global Fraud Survey: Emerging Markets Perspective,* fraudsurveys.ey.com/ey-global-fraud-survey-2018, accessed 11 March 2019.

These small incidents extrapolated across multiple stores can represent significant losses.

Online marketplace: Online trading scales up retail operations — enabling retailers to trade faster and with more people — but it also increases the risk of fraudulent activities that are damaging e-commerce. Some recent fraud trends include:

- **Listing fraud:** Employees receive kickbacks from sellers in exchange for manipulating a listing on the marketplace for higher visibility
- **Commission fraud:** Employees receive favors from sellers for reducing the commission percentage that is to be paid by the seller for sales made through an online marketplace
- **Cost arbitrage fraud:** Sellers buy their own products that have cashback offers listed on the online marketplace and then resell them offline
- **Cashback or promo fraud:** Employees inflate cashbacks and promo schemes on certain products to favor specific sellers and receive kickbacks in return
- **Click fraud:** Competitors and others deliberately click on pay-per-click (PPC) adverts (sometimes using technology) to generate fraudulent charges for advertisers, undermining the PPC campaigns. This results in driving up the advertising cost with lower conversion rates and skewed user data for online businesses
- **Listing payment fraud:** Fraudulent sellers list products for sale and request advance payment. The seller takes payment, but the product does not exist, or is not sent, and the buyers' bank or credit card details may be used as part of a wider fraud scheme

Loyalty programs: Loyalty program fraud is endemic, particularly in emerging markets. For example in Asia, where most purchases are by cash on delivery or by mobile applications, rather than a credit card. Loyalty apps record all of a customer's transactions,

including cash transactions, and collect rich customer data for retailers regarding customer choices and behaviors, including bank account and location information. This valuable data attracts hackers. Loyalty programs are also targeted by insider fraud, including abuse of points, offers and promotions, whereby employees are not passing on promotions to customers, or award themselves, and friends and family extra points, with or without a purchase, in exchange for goods or cash.

Risk management in organizations needs to consider that while risks associated with transactions are broadly similar, the scenario on the ground differs between regions, depending on cultural norms, shopping habits and levels of tech adoption. Safeguards and solutions must reflect this. For example, developed economies are seen to be experimenting with face recognition as part of the payment authorization. However, in emerging Asian economies, which are experiencing the highest growth in e-commerce, payments are mostly completed by cash on delivery, smartphone apps and prepaid cards, which are all transferable, not linked to bank accounts and do not require a credit reference.

Incidents of fraud in sales systems

Secondary sales system (distributor to retailer)
Examples of insider fraud by abuse of secondary sales system include:

- Inflated sales on new or existing retailer outlets to claim undue benefits — sales staff manipulating the system to claim incentives
- Incentives claimed by creation of "ghost salesmen" — a response to pressure for incentives and targets
- Loopholes in the retail outlet creation process that sometimes allow the creation of fake retail outlets in the secondary sales system by distributors to claim undue trade scheme benefits
- Leakage in scheme pay-outs made for inflated sales or fake retail outlets
- Database security issues around permissions enabling unauthorized access to back-end databases and work-arounds, such as sharing passwords to bypass approval workflows

Tertiary sales system (retailer to end consumer)
Examples of fraud by abuse of tertiary sales system include:

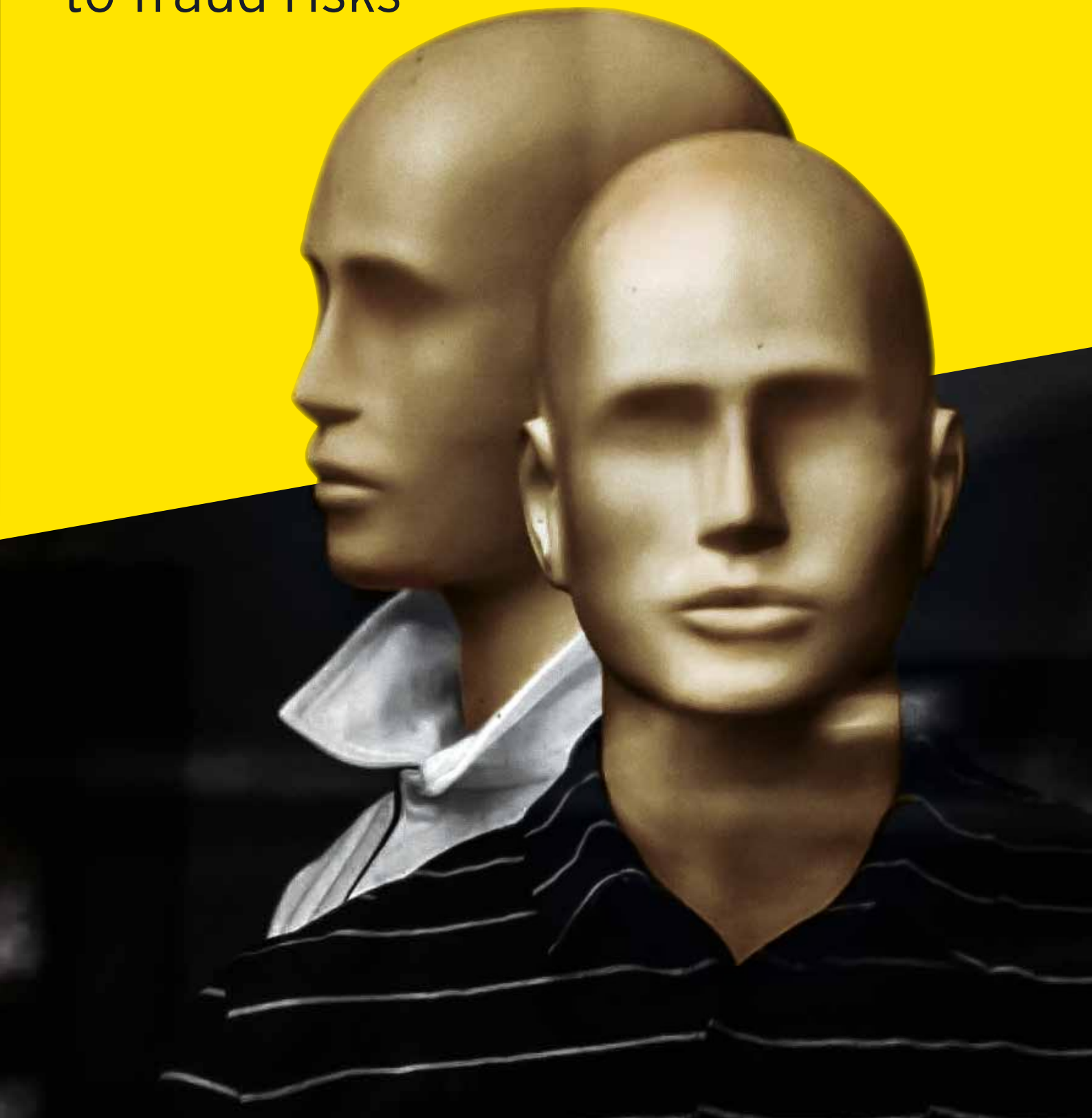
- PoS system used only for billing promotional products, thereby, transactional data not being indicative of real customer behavior
- Promotional benefits not passed on to the end consumer — the customer paying full price and the employee claiming the promotion separately (e.g., if it's two for one, they keep the extra item)
- Sales booked in non-business hours — some sales not recorded on the system
- Hackers exploiting vulnerabilities in the digital transaction platforms, including insiders who find loopholes in the system and external hackers who understand the system
- Sharing of credentials among users on site to accumulate benefits and promotions
- Misuse of reward points to claim points on customer purchases and apply them to another loyalty card (an employee's own card or one belonging to a family member or friend)

Supply chain vulnerabilities

Digitization also brings supply chain vulnerabilities. Inventory management and control systems that track and locate warehouse items, and integrate with back-office systems (accounting or enterprise resource planning (ERP)) are often in use with PoS and asset management software to monitor stock levels and movements. However, CPR organizations are reporting incidents of fraud that are exposing loopholes in secondary and tertiary sales systems (see *Incidents of fraud in sales systems*)

Drilling down into primary, secondary and tertiary sales data uncovers more specific vulnerabilities. For instance, although mobile PoS devices and DMS systems have improved visibility of transactions and stock levels, transparency levels vary depending on the software package used. Large-scale systems that deal with high volumes of transactions, particularly in Asia, may miss small incidents that are individually insignificant, but widespread across the business. Consequently, although companies are aware that there is some leakage from the secondary sales system, they are not aware of the magnitude of the overall losses.

Fix the leak: a proactive approach to assess vulnerability to fraud risks



CPR companies are spending large sums on technology transformation projects in their key business operations. It has become necessary for the key stakeholders responsible for the transformation projects to evaluate the fraud vulnerabilities that arise for the business from the adoption of new technology and practices associated with digital transformation initiatives. Specific focus is required on high-value projects that have a financial impact in

> A proactive strategy requires organizations to determine where the issues are and take steps to address them using a combination of controls, monitoring and encouragement to change behaviors.

Anurag Kashyap
Partner, EY India
Global CPR Sector Leader, Forensic & Integrity Services

Digital integrity analytics

When an organization's key risks have been identified using test scenarios and data analytics within the three-way approach above, monitoring for specific types of incidents can be incorporated into the control framework. However, considering the quantity of electronic records and transactions, which have been increasing significantly, companies face an uphill task. They need to proactively harness analytics to evaluate data, ascertain gaps and identify patterns using intuitive technology-assisted tools.

EY Forensics has an analytics platform for monitoring and managing external and insider risk. It applies a six-step process:

- Data collection and validation from all sources relevant for the organization
- Data completeness checks to ensure the quality of data obtained
- Data mapping from the client's system to the unified data model
- Data analytics based on select parameters
- Risk scoring for transactions
- Case management capability to handle the exceptions noted

This framework includes process automation to facilitate case investigations, internal audits and data management, and collaboration, which can highlight vulnerabilities and workflow improvements.

Once the risks identified are mitigated, companies must continue to monitor activities and measure the effectiveness of the anti-fraud measures. A risk management framework needs to be institutionalized to identify threats in the form of red flags. However, as the examples below demonstrate, regular independent analysis is required to uncover new loopholes and work-arounds.

Some practical examples

Forensics professionals implemented PoS data mapping and analytics to identify potential fraud in stores spread across multiple states within the US. Breaking down activities by region, store, product, type of sale (cash or card) and cashier, EY teams can identify suspicious activities ranging from pilfering – where goods or cash go missing – to large-scale leakages. An example is by identifying a spike in the number of expensive purchases being returned for a refund or multiple store cards being registered to the same address. By highlighting patterns in customer or employee behavior or unusual activities, Forensic Data Analytics can identify the possibility of an individual store or cashier being targeted by organized crime.

EY teams have developed a PoS analytics tool for a global coffee retail chain using forensic analysis to risk score activities and identify problems within stores in terms of misuse by staff. The tool runs analytics across data sets, including the number of complimentary cups and the number of staff "freebies" against the number of transactions per day. It then scores the results to identify which store present the highest risk of losing revenue through this type of staff conduct. Risk analysis is applied to geographic regions, stores, employees and transactions.

EY Forensic professsionals advised a global company in Southeast Asia, which operates a loyalty program whereby all transactions attract points that can be redeemed for cash. The high volume of data that this generates increases the potential risk of large-scale fraud. Forensic data analysis devised and conducted by EY teams confirmed that the program was indeed being misused by staff and customers. The purpose of data analysis was twofold: to plug any gaps in the system and to continuously identify red flags. The organization took action against the employees whose misuse of the

the form of incentives or payouts for company employees and external third parties involved in the value chain.

This supplements the need for a proactive strategy to detect and address loopholes in processes and systems involved in the digital transformation initiative, with a view to preventing fraud before it happens rather than reacting after the event. A proactive strategy requires organizations to determine where the issues are and take steps to address them using a combination of controls, monitoring and encouragement to change behaviors. A three-way approach to proactive forensic assessment can add value for businesses seeking to mitigate the potential leaks;

1. Identify and understand

- Identify the transformation initiative with the highest financial impact
- Understand the purpose and objectives of the transformation initiative
- Understand the key performance indicators (KPIs) linked to the transformation project that would potentially result in benefits to internal and external stakeholders, and their financial impact on the organization
- Analyze links between business-critical processes and systems involved in the transformation initiative

2. Functionality testing and data analytics

- Perform functionality testing of the system application or platform being implemented
- Design fraud risk scenarios relevant to the business processes linked to the system application or platform under focus
- Extract data from relevant sources and perform forensic data analytics to test the hypothesis for fraud risk scenarios applicable to the business
- Conduct additional checks to validate the exceptions identified based on data analytics

3. Mitigate

- Identify vulnerable areas and categorize them in order of priority
- Devise practical controls to mitigate risks
- Build a monitoring framework that helps identify red flags on a continuous basis going forward
- Assist in implementation of the controls in consultation with management
- Define and agree an ongoing review mechanism for the controls

system had been identified by this process, put in place controls to prevent such instances from recurring and subsequently changed internal processes to include ongoing monitoring and data analysis.

Proactive DMS reviews have helped multiple companies operating in developing markets identify the potential fraud vulnerabilities in existing DMS systems, operating schemes and incentive programs for general trade operations. Data analytics have helped pinpoint the exact sales behavior of outlets aimed at achieving the scheme or incentive criteria defined by the company. EY teams have also helped companies set up post-implementation monitoring frameworks to identify red flags themselves going forward.

EY proactive analysis is used to highlight a potentially fraudulent activity. Trend analytics of online sales data help spot illicit purchasing patterns, such as bulk buying and repeat returns of particular types of goods. Retrospective analytics on PoS terminals have been used to identify inappropriate or fraudulent activities, complementing the payment analytics conducted by credit card providers.

A casual dining organization in the US uses machine-learning algorithms to analyze trading and order patterns to predict which orders might be fraudulent. This fraud prevention system operates almost in real time, with the capability of flagging and preventing potential fraud before it happens.

Business intelligence tools incorporating data visualization and machine learning enable large organizations to identify trends around potentially fraudulent activities and communicate with employees who fall into the top 10%, in terms of suspicious transactions. Rather than having to discipline or dismiss individuals who are caught, it is possible to identify where the risk is in the business and proactively change behaviors. It is important to continue monitoring and measuring transaction integrity to identify which strategies and processes are making a difference, and ensure the right activities and groups are being targeted.

Conclusion and key takeaways

Digitization has transformed the CPR environment in many positive ways as e-commerce expedites almost instant trade in a wide range of products sourced from all over the world.

Successful online and omni-channel retail is highly profitable, but digitization is also opening up a different risk horizon. New threats range from cyber criminals intercepting physical and online sales systems, and dishonest or careless employees, to fraudulent third parties deliberately seeking opportunities to exploit loopholes or system work-arounds in ways that make the system vulnerable to interceptions or scams. The digitized CPR industry produces vast quantities of data, which can be leveraged to grow businesses — and protect them as well.

Today's CPR industry requires systems for identifying and combating fraud risks created by digitization. New developments in retail technology also bring new opportunities for interception and exploitation. So independent forensic analysis and measurement is needed on an ongoing basis as digital integrity is a critical success factor for any business.

How can EY help?

EY teams, with experience in forensics for the CPR sector, helps businesses develop data analytics capabilities to:

- Identify and anticipate the specific risks affecting the business
- Ensure the right controls are in place
- Monitor and analyze retrospectively and in real time

This helps create an incident plan for rapid reaction and business continuity to protect trade and reputation, should the worst happen.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

About EY's Forensic & Integrity Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG no: 003376-19Gbl

BMC Agency
GA 1011776

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/forensics