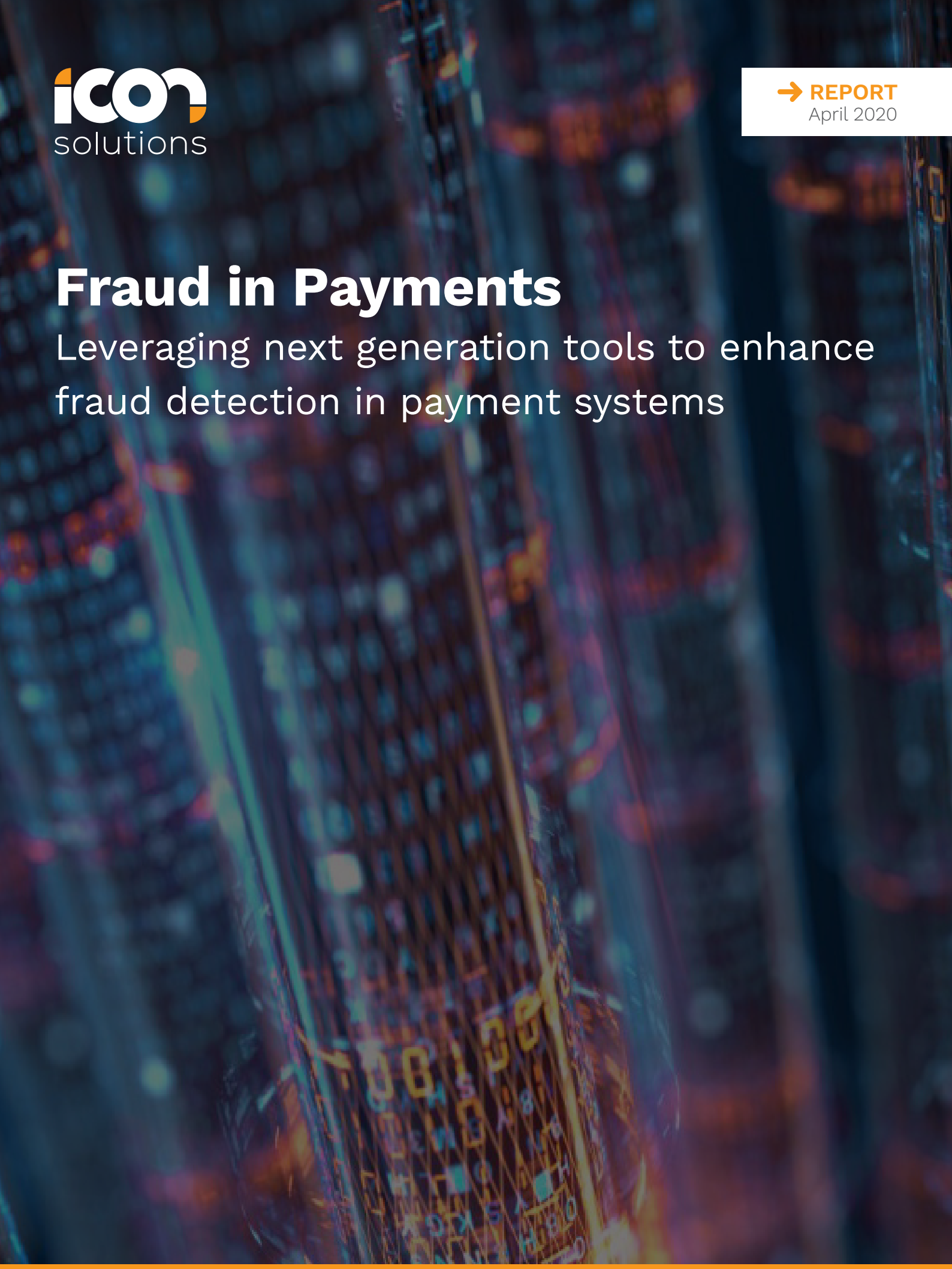


REPORT
April 2020

Fraud in Payments

Leveraging next generation tools to enhance fraud detection in payment systems

INTRODUCTION

Payments fraud continues to cost the UK Financial Services Industry in excess of £1bn per year, with the methods of attack changing in terms of their sophistication and complexity. To protect against these fraudulent incidences, banks are using several core fraud threat analytics tools to capture historic customer data (such as transaction values, transaction geographic profiles and trusted beneficiaries) to enable them to identify unusual payment behaviour and patterns. However, while these add value around the typical customer payment profile, they don't protect against the challenges presented by customer identity theft or by the hacking of customer devices. Instead, external specialist tools, also known as next generation tools, can provide the additional insight and data on the typical behaviour of 'users' and leverage their known histories to identify any unusual behaviour. By providing additional layers of information and by integrating into existing systems, these tools enable better decisions to be made as it provides payments systems with all the available datapoints to identify and prevent fraud.

This report examines these tools in more detail, how they work in practice, and the benefits they offer to fraud detection in payments.

Examining the tools available

There are currently a number of tools already on the market, common types include:

- **Device scanner solutions** which focus on the monitoring of user device types and identifiers - known devices versus new devices and the location of those devices. Once user devices (iPhones, PC's, Tablets) have been identified, the device scanner builds a database of known 'safe' devices and locations
- **Malware scanning solutions** which run scans on applications and monitor for Malware signatures on user devices and the application pages. A payload is inserted into an application to scan for Malware against a list of known threats using methods similar to anti-virus software
- **Behaviour Modelling Solution** which is a new and evolving set of tools to capture data on how a user interacts with sites (e.g. mouse velocity, keyboard usage, right mouse button usage) to build a picture of typical behaviour and journey. This data is then modelled using machine learning algorithms to decide if the user behaves the same way as their profile

These tools help identify unusual behaviour

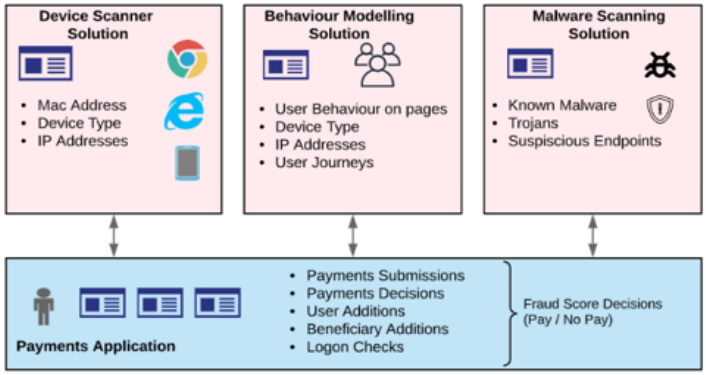
- Does the customer behaviour match previous behaviour patterns (Do they use the right mouse button, does the mouse and keyboard velocity match known values)?
- Does the device / channel used match previously used and trusted devices / channels?
- Has any Malware been introduced onto the customer devices?

➜ Addressing common threats

There are three typical threat scenarios where fraudsters will attempt to gain credentials:

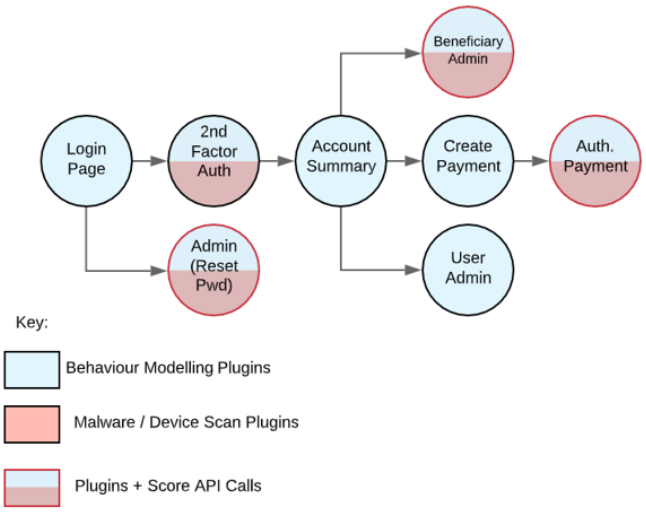
1. Malware injection to capture credentials or control applications
2. Account takeover by criminal third party
3. User credential phishing / using compromised existing client user accounts

As a result, each of the common tools mentioned earlier, specialise in specific areas:



From the application perspective, this means there is a variety of tools and providers that can be leveraged to capture complementary data from multiple tools. This data can then be analysed to provide a broad set of indicative data which will be consumed into an institution's internal Fraud and Risk Decisioning application(s). This data can then enhance data already held on transactions and other customer data.

Typically, financial institutions will use a mix of these tools to feed data to a common or suite of decisioning engine applications taking input from various sources and utilising the data in scores according to the pages / application functions accessed, as an example:

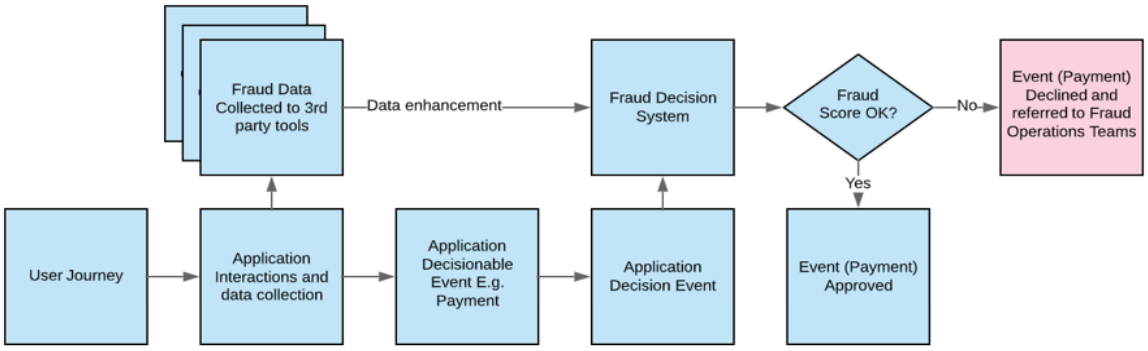


These input / plugin payloads will collect and analyse data and will be used by decisioning engines when invoked at key stages in a user journey (where a score may be required before the user can continue). Some tools will be present at every step, some, such as Malware scanners, will be initiated at the start and then again at key points of a user journey for example:

- User password reset
- Submission / approval of a payment
- Addition of a new payment beneficiary

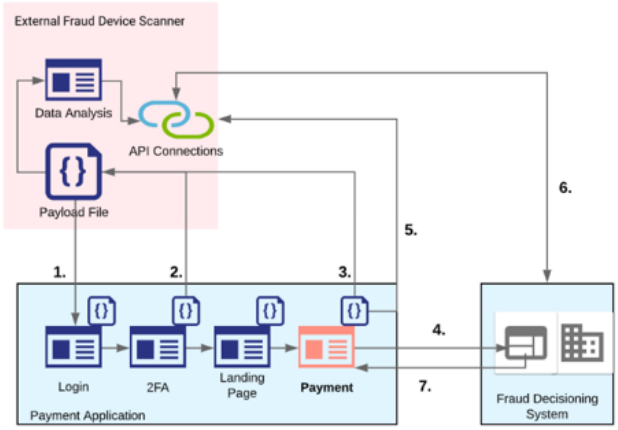
➜ Using the data in practice

The below uses an example of a payment being made to highlight how the business flow utilises the data collected by fraud tools. This data collected will inform the fraud score decision - if a score is deemed OK, then the transaction will proceed without interruption. Typically, a 'bad' or 'tentative' score will be routed to a Fraud Operations team that can contact a customer before making a final decision.



➜ Malware / Device Scan Solution integration and operation example

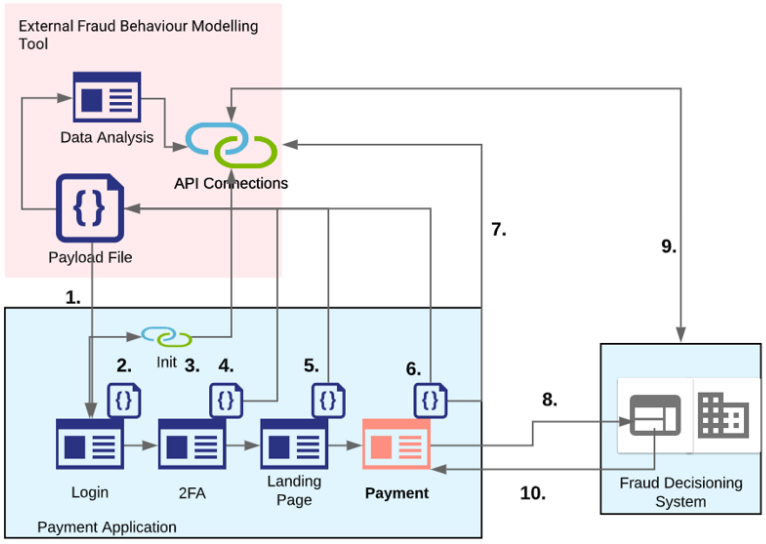
The below illustrates a typical component level operation and flow of interactions where a financial institution is using Malware / Device scanning tools to inform their fraud scores.



1. The Malware / Device scanning tool JavaScript payload is downloaded from the external fraud monitoring application into the customer application login page
2. The Malware scanning tool is activated by a function call in the page to scan the page at the two-factor authentication page collecting data on the page and storing it in the tool
3. After the user is authenticated and lands in the application as an authenticated user the user creates a new payment. The External Fraud Monitoring Tool payload performs a scan on the page initiated by a function call as the page loads and records the outcome
4. The application calls the Internal Fraud Decisioning Application to request a score
5. In parallel to step 4, an API call is made to pass the sessionID to the External Fraud Monitoring Tool to link the session in the tool to the data collected on the journey
6. The Internal Fraud Decisioning Tool makes an API call, passing the sessionID to the External Fraud Monitoring Tool and receives a score response
7. The Internal Fraud Decisioning Tool returns a score response to the application based on the analysis of data from the Fraud Monitoring Tool data and any data held in the Central Decisioning tool based on that user profile.

➜ Biometric Data Example

Biometric systems typically collect more data and operate across the whole of the user journey. The biometric system will have more interaction points so a picture can be built up of the user and the journey(s) that they make so that patterns can be monitored and identify how the user behaves within an application. Example steps shown below:



1. The Malware / Device scanning tool JavaScript payload is downloaded into the customer application login page. The payload will start to track the following:

    a. User sessionID

    b. User behaviour patterns (by communicating back to the product data collection points using call-backs)

2. The payload sets the page 'context' per the value set in the application page (usually by a tag in the page). The 'context' is generally something describing the page name (e.g. login, 2FA, landing screen) and is called via a function call in the payload

3. The init call will be made via an API call to the External Fraud Tool system so that the sessionID and the user ID value are linked for tracking purposes. The sessionID of the user and a user ID (usually obfuscated by hashing an existing ID to maintain a consistent value unique to that user e.g. user ID might be 100045, hashed value would be 37d0f121db69fd09f364df89e4405e31). This is used to record all sessions and journey data generated by this user

4. The user moves to a new page, the "context" of the new page is recorded e.g. "2FA" for two-factor authentication via a function call in the payload and is recorded in the External Fraud Tool system. In addition, the user behaviour is captured as they interact with the page and recorded in the External Fraud Tool system

5. The user moves to a new page, the "context" of the new page is recorded e.g. "landing page" for the post login landing page via a function call in the payload and is recorded in the External Fraud Tool system. In addition, the user behaviour is captured as they interact with the page and recorded in the External Fraud Tool system

6. The user moves to a key page, such as a payment page. Again the "context" and behaviour are tracked as normal

7. In addition, on submission of the payment a further API call will be made giving the hashed user ID, sessionID, and a 'score' event trigger. This will prompt the External Fraud Tool to analyse the user session

8. In parallel, a call will be made to the existing Internal Fraud Scoring Application as part of normal operation

9. The Internal Fraud Scoring Application will call out via an API call passing the user ID and session ID of the session related to the payment being made, the response to this call will be a score based on how the External Fraud System evaluates that user session against expected behaviours

10. The Internal Fraud Scoring application will use the additional score parameters returned from the External Fraud System(s) to reach a decision on whether the payment can proceed. This score will then be returned to the application.

➜ The benefits of many

In the modern application-based payments industry it is clear that a mixture of Malware, Device Scanning and Biometric tools is needed to really address the threat of fraud in payments. Using a combination of these tools will provide additional data on user behaviour and journey to existing Fraud Threat Scoring tools, which will enhance and increase the reliability of payments decisions.

In order to leverage these new tools, financial institutions should review their payments application architecture and toolsets. They should look to outwardly integrate their core fraud decisioning platforms and engineer these systems to enable a flexible and open integration pattern to these tools to improve detection rates.

Typically, this will involve:

- Building in an index or catalogue of pages / key application 'decision points' to enhance data captured and allow analysis of the 'customer journey' through the site / application
- Opening up to external vendor systems using API's with Cloud endpoints (to integrate with third party suppliers) using REST API patterns
- Implementing real-time score calls to gather third party supplier 'scores' and integrate those with existing decision tool

Further reading around individual tools can be found below as examples.

Biometric Data Tool (Biocatch) = https://www.biocatch.com/

Device Scanning Tool (ThreatMetrix) = https://risk.lexisnexis.com/corporations-and-non-profits/fraud-and-identity-management

Malware Scanning Tool (Trusteer) = https://www.ibm.com/uk-en/security/fraud-protection/trusteer

Tag Management (Tealium) = https://go.tealium.com/

ABOUT ICON SOLUTIONS

Icon Solutions is a fintech partner providing world class payment and enterprise solutions to the global financial services sector. Clients include leading international institutions such as BNP Paribas, Citi, HSBC, Lloyds Banking Group and Nationwide. Whether it be assessing payments systems, producing transformation roadmaps, or simply providing subject-matter expertise, Icon enables clients to be leaner, innovative, and responsive to the demands of the future.

icon solutions

LEARN MORE

iconsolutions.com | info@iconsolutions.com | iconsolutions