Stop application fraud without disrupting your good customers

Application fraud prevention with Hunter and CrossCore™

The fraud challenge

Application fraud continues to rise

Improvements in online application processing have meant greater convenience for customers and improved operations for companies. However, these online channels have also opened up new opportunities for fraud attacks – now more than ever. Fraudsters focus on online applications, with 88% of identity frauds being Internet-enabled.

Customers abandoning applications directly affects top-line growth

Fraud managers today often must reduce fraud losses with minimal staff and resources, while at the same time avoiding negatively impacting the customer experience.

Your organisation needs to keep pace with fighting increasingly complex fraud

Fraud teams have to continually work smarter. Data and analytics from multiple systems need to be integrated together onto a common platform and a single tool-set. Investigators need access to the broadest array of identity and fraud capabilities, in a rapid and intuitive investigation environment.

63% of businesses report experiencing the same or more fraud losses in 2017 compared with 12 months ago

Fraudsters focus on online applications, with **88%** of identity frauds being Internet-enabled.
30 legitimate customers are challenged or blocked to catch **1** fraudster

Introducing Hunter, a complete application fraud management solution

Flexible, scalable, and future proof

Hunter is an application fraud management solution that fights fraud every day for our clients around the world. It seamlessly integrates with your existing application processing system, as well as with complementary fraud tools like device intelligence and behavioural biometrics for application screening on the CrossCore™, Experian's smart, open fraud and identity platform. To counter complex and evolving fraud, Hunter offers a high level of configurability to match and profile application data – with tools that enable quick decisions and analysis of connected fraud rings. And as you look to add new application fraud tools, Hunter can integrate with what you need through the CrossCore platform.

Application fraud risk engine

Hunter screens application data in real-time to check for potential data manipulation and anomalies which could indicate fraud. In addition, it looks for connections to previous suspected and known fraudulent applications, and screens against available fraud intelligence sources, applying proven and flexible fraud risk rules. Hunter then generates a fraud score that indicates the likelihood of fraud and is used to prioritise referrals.

Data consortia

Where available*, Hunter's data-sharing schemes offer an answer to the shared problem of fraud, cross-matching data across organisations, corporate groups and industries. In addition to a significant increase in fraud detection, participants in our data-sharing schemes also often report a reduction in fraud attack rates, as fraudsters avoid the consortium's members entirely.

Fraud investigation

Hunter's sophisticated workbench and feature-rich case management tools are used to investigate and record fraud. And Hunter's visualisation tools graphically display the links between matched items, providing your fraud referral teams with a clearer view of links between connected applications.

Clients who participate in Hunter's national fraud data-sharing schemes typically achieve at least a **45%** improvement in fraud detection compared to only screening against their own data

*Please check with your sales or account manager for availibility in your country.

Identifying good customers and stopping fraudsters

Detect application fraud

Hunter uses a core set of proven fraud detection rules to screen applications. This rule set is completely flexible and can be configured for different services and types of fraud depending on your requirements and risk tolerance. Rules can be rapidly amended as fraud profiles and products change, offering total coverage for your organisation. Additionally, Hunter screens application data and verifies against available external data sources to highlight matches with known fraud information, and inconsistencies against previous genuine applications.

Visualise linkages to expose fraud patterns

Hunter's visualisation tools graphically display the links between matched items, providing your fraud referral teams with a clearer view of the way information is linked. This often provides a picture of the wider fraud risk exposure, that would otherwise not be so apparent from just viewing rules. It is a key tool for identifying organised fraud and fraud rings.

Investigate fraud

Hunter offers your fraud investigators a wide range of tools to assist in the investigation of a suspicious case. Referred applications are displayed to your team in flexible, configurable work queues ranked by fraud risk and allocated to investigators based on your operational requirements. Your investigators can review the application, interrogate the data, and explore anomalies using powerful search and comparison tools, and carry out a range of investigative and verification activities. When the investigation is complete, the outcome is recorded for immediate use in the on-going detection process and for monitoring and analysis. Retrospective rules identify links between the marked application and any previous applications, flagging them for investigation, further enhancing your fraud detection capabilities. Once these actions are complete, this decision gets passed back to the application processing system.

Benefits of Hunter

- **Improve your fraud detection and avoid accepting fraudulent applications**

- **Reduce false positive referrals, ensuring a good experience for good customers**

- **Focus on your highest risk applications in order of priority, maximising return on your operational costs**

- **Keep pace with changes in fraud with flexible fraud rules**

- **Add innovative fraud tools for a strong layered defense**

Data matching with industry and national schemes

The growth of data consortia worldwide is a testament to how effective they are at preventing fraud. When one consortium member encounters a new fraud attack, that information is immediately available to the rest of the consortium. The systems operate on a principle of strict data reciprocity. Client experience has shown that data-sharing offers significant advantages in detecting higher volumes of fraud. Participants in national fraud data-sharing schemes using Hunter typically achieve at least a 45% improvement in fraud detection compared to only screening against their own data.

Manage system and team performance

Integrated management information and reporting enables you to evaluate system performance and your fraud prevention team's efficiency. Through analysing fraud trends and patterns, now you can evaluate and fine-tune detection rules as well as quantify the value of fraud prevented. In addition, when a fraud is detected for an existing customer, this information can be fed back into the system to further enhance future checking and continually improve your detection and accuracy rates.

Monitoring is a crucial part of the fraud prevention process. Criminals are continually changing their methods of attack and as a result fraud prevention measures can lose their effectiveness over time. Management information and the Hunter dashboard allow constant monitoring to control the quality, accuracy and efficiency of the detection process.

Business Support and Optimisation (BSO)

Our BSO team of experts will work closely and collaboratively with you, with regular discussion around performance, key performance indicators (KPIs) and fraud trends. Your allocated BSO resources will regularly review the effectiveness of your data / solution and provide pro-active recommendation for continuous improvement.

By monitoring matches and outcomes, they are able to identify those rules and referral strategies that are most effective for your business. BSO resources will pro-actively suggest changes to your rule strategy. As new rules and fraud intelligence are developed, they work with you to ensure your fraud strategy makes use of the most up-to-date and effective rules available.

The wider configurable functionality of Hunter also plays a key part in ensuring an optimal fraud strategy. As each new release of the Hunter product becomes available, your BSO team will work with you to quickly utilise new features that are expected to immediately provide value to your business.

Clients who regularly collaborate and engage with our BSO teams typically see significant increases in fraud finding and improved operational efficiencies.

Hunter is trusted by clients around the world

You don't have to take our word for why Hunter is the right choice for stopping application fraud. Hunter is used by over 300 organisations in 22 countries. Our Hunter clients represent a wide range of industries, including banking and financial services, insurance, telecommunications, automotive, utilities, commercial finance and retail. We save our clients an estimated **three billion U.S. dollars annually** from prevented fraud losses.

Help ensure that your fraud team has the tools, expertise and support on hand to respond quickly as fraudsters change tactics

Hunter is trusted by over **300** organisations in **22** countries to mitigate their application fraud

Expand Hunter's value with the CrossCore™ Fraud and Identity platform

CrossCore is a smart, open fraud and identity platform. It delivers a future-proof way to modify fraud strategies quickly, catch fraud faster, improve compliance and enhance the customer experience. For application fraud detection in CrossCore, we start with Hunter as a foundation, and then include additional fraud tools that are quickly integrated to address.

Why is CrossCore different?

CrossCore combines a flexible, scalable API with powerful workflow and decisioning strategy capabilities. That means:

- You have common access to your tools in CrossCore through a flexible API. This lets you test and add new systems much more quickly than through traditional integration approaches.

- CrossCore uses a powerful and flexible workflow and decisioning strategy design so that you can use your various fraud and identity systems when and where you need them – down to the transactional level.

- Your fraud team can connect and optimise a portfolio of best-in-class solutions — including Experian and other partners — with your existing systems.

Additional fraud tools now available with Hunter via CrossCore*

- Device intelligence

- Behavioural biometric application monitoring

- Identity document verification

- Email risk scoring

- Mobile phone verification and phone data intelligence

- Synthetic identity checking

- Advanced machine learning services

* Check with your sales or account manager for availability of specific tools in your region.

Optimising your fraud solution

Consulting is at the heart of every delivery by Experian
Our consultants have extensive experience in the fraud industry, analytics and product deployment. They will work with you at every stage of the project. First, they work to fully understand your business and strategic direction. Then they help to design and implement systems and processes that to deliver objectives.

Experian consultants help analyse and identify the improvements in fraud avoidance, prevention or detection to be expected post-implementation, enabling you to invest with confidence, knowing the return on investment makes sound commercial sense.

Advanced machine learning takes fraud detection to new heights
Now available through the CrossCore platform, Experian's machine learning can develop client-specific models that optimise fraud detection and minimise referrals based on your specific data. Our machine learning services utilise methods including structured and unstructured machine learning modeling, deep learning, and decision trees. Data scientists test to find the right combination of methods and create a hybrid approach. With CrossCore, you can bring data from different systems together. Greater diversity in data sources significantly improves the accuracy of your model and fraud detection.

Hunter is an application fraud management solution that seamlessly integrates with your existing application processing system. It works with complementary fraud tools available through CrossCore™ like device intelligence and behavioural biometrics for enriched fraud detection and investigation.

To learn more about how you can improve your fraud detections, visit www.experian.co.za

www.experian.co.za