LexisNexis®
RISK SOLUTIONS

CRIFBÜRGEL Helps Customers to Make More Informed Risk Decisions with Dynamic Digital Identity Intelligence from LexisNexis® ThreatMetrix®

KEY FEATURES OF THE PARTNERSHIP

Partnering with LexisNexis® Risk Solutions, CRIFBÜRGEL is able to enrich its own static identity data with dynamic, near real-time digital identity intelligence. Bridging the physical and digital divide, CRIFBÜRGEL has enhanced its identity verification and credit check solutions with intelligence from LexisNexis® ThreatMetrix®. Partnering with LexisNexis Risk Solutions enables CRIFBÜRGEL customers to:

- Leverage the LexisNexis® Digital Identity Network®, tapping into global shared intelligence from millions of daily end user interactions, to reliably differentiate fraudsters from trusted end users in near real-time.

- Leverage LexID® Digital and go beyond device-based analysis, bridging offline and online data for each transacting end user.

- Enhance detection of stolen identity credentials in near real-time, reducing fraud losses.

- Minimize friction for trusted end users.

BOTTOM LINE

Digital identity intelligence from the ThreatMetrix solution augments CRIFBÜRGEL's identity verification and credit check solutions, supporting its customers to identify high-risk scenarios in near real-time. The CRIFBÜRGEL/ LexisNexis Risk Solutions partnership has enabled additional risk intelligence data to be integrated into fraud and risk decisions across digital businesses in Germany and the wider EMEA market.

"Validating end user identities has become a three-dimensional challenge. CRIFBÜRGEL can't just rely on static identity data: fraudsters can now steal or buy this same data. LexisNexis ThreatMetrix leads the field with the dynamic nature of its intelligence. It gives us the near real-time edge we need to provide more reliable risk assessments."

–CRIFBÜRGEL

Overview

CRIFBÜRGEL specializes in credit information systems, business information and credit management solutions. Established in 1988, CRIFBÜRGEL has become one of the leading providers of credit information with more than 6,300 banks and financial institutions, and 55,000 business clients using CRIFBÜRGEL services in 50 countries on a daily basis.

Today, CRIFBÜRGEL specializes in tailored solutions for credit assessment, fraud prevention and address management. The company has exceptional industry expertise in e-commerce, payment services, telecommunication and receivables management in particular.

CRIFBÜRGEL's mission is to help businesses perform better, making lending more efficient and effective with the most reliable credit information. This approach relies on integrating the best possible data, both static and dynamic, so that businesses can make more informed risk decisions.

"The integration of ThreatMetrix digital identity data into our existing credit risk and identity decision platform brings a strong added value for our customers."

–CRIFBÜRGEL

Fighting Fraud and Empowering Risk Decisioning Across the Online Customer Journey

The dark web marketplace always has an abundance of stolen identity credentials, with global data breaches fuelling the stolen identity trade. Cybercriminals can buy stolen identity credentials and use the data to build near perfect replicas of genuine identities that are used to perpetrate fraud.

"Synthetic identities can be extremely hard to detect," said Kai Wanka, Head of Fraud Solutions at CRIFBÜRGEL. "A fraudster can appear legitimate when using a stolen or fabricated identity, sometimes even passing static verification checks. We needed to look beyond isolated pieces of information and really understand how trusted end users behave. Device spoofing, location spoofing or unusual transaction behavior were key indicators of high-risk behavior."

Consumer behavior is increasingly complex and multifaceted, transacting across channels, devices, and locations. The key to detecting synthetic identities is having the ability to analyze the various pieces of information an individual creates as they go about their daily lives, both on and offline. Businesses then need the ability to understand the links between those seemingly disparate pieces of information to recognize and understand patterns that show how consumers' identities develop and transact.

CRIFBÜRGEL sought a partnership which would unite online and offline intelligence, providing its customers with near real-time digital intelligence on transacting end users. In bringing together static and dynamic identity intelligence, CRIFBÜRGEL wanted to augment its identity verification and credit check solutions and provide customers with reliable fraud and risk insights around the legitimacy of a digital identity. For CRIFBÜRGEL, it was imperative that their customers were able to build trust with genuine, good consumers, with the combined static and dynamic intelligence empowering them to make the right decision at different points in the online user journey, be it login, payment or new account application.

"We needed to go beyond device intelligence – it's just not enough when the digital footprint of consumers is getting more complex every day. We always want to empower our customers by giving them the best intelligence, and with intelligence from LexisNexis ThreatMetrix, we are able to paint a more reliable picture of who our customers are transacting with."

–Kai Wanka, Head of Fraud Solutions, CRIFBÜRGEL

The Power of Global Shared Intelligence to Detect Stolen Identity Credentials in Near Real-time

Digital identity intelligence from the ThreatMetrix solution is collected and processed by the LexisNexis® Digital Identity Network®, a network of global shared intelligence from millions of daily consumer interactions including logins, payments and new account applications.

This intelligence is brought to life by LexID® Digital, helping businesses elevate fraud and authentication decisions from a device to a user level, as well as unite offline behavior with online intelligence. LexID Digital is comprised of a unique digital identifier, a trust score and a visualization graph for each connecting user, which together act as a benchmark for the integrity of current and future transactions. For CRIFBÜRGEL, LexID Digital enables the consistent identification of an end user, irrespective of changes in device, locations or behavior. Intelligence from the Digital Identity Network helps reliably recognize the same returning user behind multiple devices, email addresses, physical addresses and account names.

"We can now help our customers better identify trusted end users," said CRIFBÜRGEL's Kai Wanka. "The intelligence from LexisNexis ThreatMetrix, combined with our own data, allows our customers to really see the bigger picture when it comes to their end users."

The digital identity intelligence from the ThreatMetrix solution enabled CRIFBÜRGEL to adapt and tailor services to different customer demands across the online user journey. For example, a German supermarket wanted to streamline the online Card-Not-Present (CNP) checkout experience. The combined intelligence from CRIFBÜRGEL and LexisNexis ThreatMetrix allowed the supermarket to:

- Minimize friction and expedite the checkout experience for trusted end users.

- Reduce fraudulent payment transactions.

- Differentiate fraudsters from genuine end users in near real-time.

> **"Partnering with LexisNexis® Risk Solutions has seen the physical and digital realms come together – with the combined approach allowing us to secure payments and make lending more efficient with the most reliable fraud and risk intelligence."**
>
> –**Kai Wanka,** Head of Fraud Solutions, CRIFBÜRGEL

Harnessing Global Shared Intelligence to Protect Against Synthetic Identities and Stolen Identity Credentials

LexID Digital bridges online and offline data elements for each transacting user and goes beyond device-based analysis, grouping various other entities such as tokenized email addresses, physical addresses and credit card hashes based on complex associations formed between events. This enables LexID Digital to consistently identify a person irrespective of changes in devices, locations or behavior.

ThreatMetrix SmartID® identifies returning users that wipe cookies, use private browsing, and change other parameters to bypass device fingerprinting. Derived from the analysis of many browsers, plug-ins, and TCP/IP connection attributes, SmartID improves returning user detection and reduces false positives.

ThreatMetrix Smart Analytics provides a clear-box approach to behavioral analytics and machine learning. Smart Analytics generates dynamic profiles matched to individual user behavior and uses these to build more accurate, yet simpler, risk models. The result is a competitive edge in customer experience with reduced false positives, whilst maintaining the lowest possible fraud levels.

Deep connection analysis technologies give CRIFBÜRGEL a clearer view of suspicious events. Fraudsters often attempt to hide behind location and identity cloaking services such as hidden proxies, VPNs and the TOR browser. With proxy piercing technology, the ThreatMetrix solution examines TCP/IP packet header information to expose both the Proxy IP address and True IP address.

LexisNexis®
RISK SOLUTIONS

For more information,
call 866.528.0780 or visit risk.lexisnexis.com/FIM-EN