goHenry Ltd – Job Specification for Fraud Analyst

Full Time Permanent Position

Location – Farnborough, Hampshire

Salary £23 - £25k 37.5 hour week – Monday -Friday

Reporting to Head of Ops & Member Services goHenry Ltd.

goHenry is a dynamic, fast-growing business in the FinTech sector providing a web and mobile based prepaid debit card solution for families, children and teenagers to address the lack of financial products for this market in an increasingly cashless society. Listed in KPMG's Top 100 FinTech companies, our aim is to provide an engaging framework for young people to develop money skills with parental controls thereby encouraging earnings, savings and spending within a safe environment.

We enable more than 150,000 families to handle their pocket money online via our website www.gohenry.co.uk and the goHenry mobile app. Parents load their account via either debit card or bank transfer and can make automated weekly pocket money payments, set tasks for their children, savings targets and invite relatives to be part of the child's financial education. The children are able to earn, save and spend within the limits set by the parent on the account.

We have an in-house risk assessment programme running across our systems protecting against fraud both on the loading of the parent account via debit card payment and also the spending via the goHenry Visa Pre-Paid Debit Card. As we are now in a period of sustained and substantial growth, this system needs to be constantly refined. We are therefore seeking an enthusiastic, analytical individual to help us improve and build on the protection of the goHenry service going forward.

Responsibilities:-

- Review and analyse on-line payment transactions to identify any potential fraudulent activity
- Make accept/decline account applications flagged for manual review within agreed SLA
- Liaise with Customer Service Team – It will be this team offering support to the daily fraud monitoring processes.
- Analyse Member debit card loads by using data mining solution and other tools to identify potential fraud or compliance issues
- Investigate in depth all cases of actual or suspected fraud and non-compliance
- Utilise data intelligence reporting effectively to identify and analyse risk
- Work with the Ops Controller to regularly review and propose solutions to improve our processes to minimise the risk of fraud
- Review and defend all chargeback transactions
- Respond to Bank and Police requests for information and assist with investigations into fraudulent activities
- Monitor all balance adjustments made by staff members to member accounts to ensure authorised correctly
- Liaise with our payment partners as required to ensure risk tools being used effectively by goHenry

Ltd.
- Working with Ops Controller to provide the business with reports and updates fraud – weekly, monthly and as and when required
- Follow agreed communications plan with other departments and communicate as required in order to achieve fraud and payments strategy
- Support and assist Head of Operations on all reporting and analysis
- Upskill and provide coaching for goHenry Member Service Operators and new starters as required

Candidates should have the following skills and be able to demonstrate the following:
- An understanding of the demands of working for a fast paced, online company with the requisite need for a flexible approach and the ability to respond to Business needs
- We will be looking to expand internationally and therefore online fraud experience working for an international ecommerce company would be preferable
- Knowledge and experience with tools and techniques used to identify and prevent online fraud
- Strong analytical skills and attention to detail – ability to spot trends and identify unusual patterns of behaviour
- Excellent interpersonal and communication skills
- High level of PC literacy – particularly in Microsoft Excel & Word (Office)
- Ability to plan, organise and prioritise work under pressure to meet deadlines
- Ability to use own initiative and work well as part of a team
- Able to display a high degree of confidentiality and discretion

The below is highly desirable:
- Experience of using a data-mining solution to identify store fraud and non-compliance
- An understanding of online payment processing and fraud prevention processes, including chargebacks
- Knowledge of the Payment Card Industry (PCI) Data Security Standard (DSS) regulations
- Experience with SQL and/or analysing large amounts of data.